UNIVERSIDADE DO SUL DE SANTA CATARINA
LEANDRO JAMIR SILVA

TRABALHO DE CONCLUSÃO DE CURSO:
INTERNET DAS COISAS.

Palhoça
2017

LEANDRO JAMIR SILVA

TRABALHO DE CONCLUSÃO DE CURSO: INTERNET DAS COISAS.

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia Elétrica e Telemática da Universidade do Sul de Santa Catarina como requisito parcial à obtenção do título de Bacharel em Engenharia Elétrica.

Orientador: Prof. Glauco Ligeiro.

Palhoça

2017

LEANDRO JAMIR SILVA

TRABALHO DE CONCLUSÃO DE CURSO:
INTERNET DAS COISAS.

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de Bacharel em Engenharia Elétrica e aprovado em sua forma final pelo Curso de Engenharia Elétrica e Telemática da Universidade do Sul de Santa Catarina.

Palhoça, 01 de dezembro de 2017.

Professor e orientador Glauco Ligeiro. Eng.
Universidade do Sul de Santa Catarina

Professora Sheila Santisi Travessa, Dra. Eng.
Universidade do Sul de Santa Catarina

Profissional Ricardo Scheidt, Eng.
Universidade do Sul de Santa Catarina

À Mireli da Cunha, pessoa com quem amo partilhar a vida. Com você tenho me sentido mais vivo de verdade. Obrigado pelo carinho, a paciência e por sua capacidade de me trazer paz na correria de cada semestre.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado saúde e força para superar todas as dificuldades e concluir o ciclo universitário.

Aos meus pais e irmãos, pelo amor, incentivo e apoio incondicional.

Ao meu orientador, Glauco Ligeiro, por apostar em mim e pela disponibilidade e todo auxílio prestado.

A professora, Sheila Santisi Travessa, pela compreensão, apoio e confiança.

A Universidade do Sul de Santa Catarina, pela oportunidade de fazer o sonhado curso de engenharia elétrica em horário compatível ao horário de trabalho.

A todos os meus amigos e familiares pela compreensão nos momentos de minha ausência dedicados ao estudo superior.

E a todas as pessoas que contribuíram de uma forma ou outra em minha formação tanto pessoal como profissional bem como no termino deste trabalho de conclusão de curso.

A todos meu muito obrigado.

“A persistência é o caminho do êxito.” (Charlie Chaplin).

RESUMO

Atualmente estar ligado à Internet é muito mais do que simples conectividade e transporte de mensagens. A maior rede do mundo é aberta e pessoas estão constantemente acrescentando coisas a ela e é natural que eles queiram que as coisas interajam de uma maneira ligeiramente automática. Diariamente uma variedade de soluções de comunicação entre essas coisas surge. Ideias como a popular cidade inteligente, por exemplo, puxam um grande número de domínios específicos como Transporte, Energia, Meio Ambiente, Vida Assistida, a maioria sempre pré-fixados com o termo "Inteligente" para enfatizar o fato de incorporarem uma espécie de inteligência e consciência global. Porém a grande maioria das soluções são voltadas para domínios de aplicação específicas com arquiteturas específicas, com pouco espaço para troca de dados com outros sistemas e interoperabilidade. A Internet das Coisas visa esta interoperabilidade. Infelizmente por ser aberta a Internet também esta sujeita a pessoas mal intencionadas que tentam sempre tirar proveito e por isso entre os mais importantes desafios da Internet das Coisas esta à segurança, incluindo identidades, autenticação e autorização para que uma comunicação maquina-maquina possa continuar funcionando mesmo submetidas a eventos ou pessoas que possam de alguma forma querer atacar ou dificultar por bel prazer ou interesse.

Palavras-chave: Internet das coisas. Aplicações. Segurança. Desafios.

ABSTRACT

Currently being connected to the Internet is much more than simple connectivity and messaging. The largest network in the world is wide open and people are constantly adding things to it and it is natural that they want things to interact in a slightly automatic way. Every day a variety of communication solutions among these things emerges. Ideas such as the popular smart city, for example, bring a large number of specific fields such as Transportation, Energy, Environment, Assisted Living, most always pre-fixed with the term "Intelligent" to emphasize the fact that they incorporate a kind of global intelligence and awareness. However, the vast majority focus on specific application domains with specific architectures, with little place left for data exchange with other systems and interoperability. The Internet of Things is aimed at this interoperability. Unfortunately for being an opened environment the Internet is also subject to malicious people who always try to take advantage. Therefore among the most important challenges of the Internet of Things this the security, including identities, authentication and authorization so that an M2M communication can continue to function even under events or people who may somehow want to attack or hinder for pleasure or one's interest.

Keywords: Internet of things. Applications. Safety. Challenges.

LISTA DE ILUSTRAÇÕES

Figura 1 – Arquitetura genérica de IoT proposta por Zarghami 16
Figura 2 – Arquitetura de sistema de nuvem para IoT 17
Figura 3 – Arquitetura básica oneM2M 18
Figura 4 – Arquitetura funcional oneM2M 19
Figura 5 – Arquitetura proposta pela IoT-A 20
Figura 6 – IoT tecnologias subjacentes 21
Figura 7 – Etiqueta RFID 22
Figura 8 – Infográfico da Harbor Sensores 22
Figura 9 – SensorHub da IoTerop 25
Figura 10 – Arquitetura publish/subscribe MQTT 29
Figura 11 – Alguns domínios de aplicações de IoT 32
Figura 12 – Amostra de algumas aplicações de IoT na indústria 35
Figura 13 – Capacete de proteção inteligente startup Americana DAQRI 36
Figura 14 – Áreas de aplicações IoT em cidades 37
Figura 15 – Infográfico da Smart City Santander, Espanha. 39
Figura 16 – Sensores em dispositivo fitness portátil 40
Figura 17 – Dispositivos de tecnologias portáteis 41
Figura 18 – Dispositivo de tecnologia não portátil 43
Figura 19 – Monitores de saúde domésticos 44
Figura 20 – Representação de nano robôs autônomos 45

LISTA DE GRÁFICOS

Gráfico 1 - Análise do McKinsey Global Institute 24
Gráfico 2 - Potencial econômico de aplicações de IoT 33
Gráfico 3 - Valores do benefício do bem estar 42

SUMÁRIO

1 INTRODUÇÃO 12
1.1 JUSTIFICATIVA 12
1.2 OBJETIVOS GERAIS 13
1.3 OBJETIVOS ESPECÍFICOS 13
1.4 METODOLOGIA DE PESQUISA 13
1.5 DELIMITAÇÃO DO PROBLEMA 14
1.6 ESTRUTURA DO TRABALHO 14
2 DEFINIÇÃO DE INTERNET DAS COISAS 15
2.1 ARQUITETURA DA INTERNET DAS COISAS 15
2.2 ELEMENTOS 21
2.3 INTERAÇÕES TECNOLÓGICAS 23
3 DESAFIOS DA INTERNET DAS COISAS 26
3.1 REGULATÓRIO 26
3.2 PROTOCOLOS 27
3.3 SEGURANÇA 31
4 APLICAÇÃO DE IOT 32
4.1 APLICAÇÕES INDUSTRIAIS 34
4.2 APLICAÇÕES EM CIDADES 36
4.3 SAÚDE HUMANA 40
4.3.1 Wearables 41
4.3.2 Non-wearable 42
4.3.3 Implantables 44
5 CONCLUSÃO 46
REFERÊNCIAS 47

1 INTRODUÇÃO

A internet das coisas está rapidamente ganhando espaço em cenários de tecnologias de comunicação modernas e basicamente visa interligar nossa vida cotidiana a objetos que utilizam a internet como meio de comunicação. Essa interconexão de dispositivos na internet, chamada Internet das Coisas (IoT, do inglês Internet of Things), possibilitará que tais dispositivos sejam utilizados remotamente por humanos ou até mesmo por outros dispositivos, (Tan e Wang, 2010). Segundo Tan e Wang, desta maneira a Internet das Coisas é uma nova forma de tecnologia da informação e da comunicação que se difere da habitual, onde pessoas se comunicam com outras pessoas pois agora as coisas também poderão se comunicar com as pessoas e com outros dispositivos. (Tan e Wang, 2010).

De acordo com KEYSIGHT Technologies, em 2020, a "Internet das coisas" irá conectar 50 bilhões de dispositivos que podem transmitir dados úteis e informações de controle através de uma rede de sensores. Desta forma este tipo de comunicação acabará se tornando a próxima geração da Internet, sendo conceituada como uma rede mundial de objetos interconectados. (Jiang, 2013). Ainda em 2020, segundo o ministro das comunicações, André Figueiredo (PDT), terá o surgimento da tecnologia 5G que é considerada um importante bloco de construção para a consolidação da “Internet das Coisas”. Logo após assinar um acordo de cooperação com a União Europeia para o desenvolvimento da tecnologia 5G, em fevereiro de 2016, o ministro André Figueiredo (PDT) lembrou: “Isso não significa que ferramentas estejam operativas apenas em 2020. É uma evolução gradativa até que estejam prontas comercialmente para a população”.

1.1 JUSTIFICATIVA

A IoT representa a primeira evolução real da Internet, tendo um grande avanço na capacidade de coletar, analisar e distribuir dados. Ela representa um avanço que levará ao uso de aplicações revolucionárias. (Evans, 2011). O número de aparelhos como tablets, telefones inteligentes, computadores pessoais, laptops, PDAs e mesmo outros dispositivos embarcados portáteis conectados à Internet está aumentando e uma grande parte desses dispositivos móveis incorpora diferentes sensores e atuadores que podem detectar, tomar decisões inteligentes, executar cálculos e transmitir informações coletadas úteis pela Internet (Zhou e Zhang, 2011). Uma rede de tais dispositivos com diferentes sensores pode dar origem a inúmeras aplicações

surpreendentes e serviços que podem trazer significativos benefícios pessoais, profissionais e econômicos. (Li e Huang, 2011).

A internet das coisas traz a possibilidade de objetos comuns como automóveis, cancelas de estacionamento e celulares, conectarem-se entre si remetendo informações sobre o que acontece à sua volta e favorecendo cada vez mais a adoção de ferramentas que ampliam a participação, como afirmou Paula Faria idealizadora do Connected Smart Cities realizado no Brasil: "Algumas cidades usam aplicativos para que motoristas avisem sobre buracos na rua, outras, para que surfistas contribuam indicando a qualidade de água do mar".

Por ser um cenário complexo em uma área repleta de novidades a cada momento ele merece um estudo descritivo para situar hoje como estas novas tecnologias irão afetar nossa vida em 2020 ou mesmo antes uma vez que a cada dia estas se tornam cada vez mais presentes.

1.2 OBJETIVOS GERAIS

Realizar um estudo de tendência sobre IoT para uma melhor compreensão e apresentar IoT definindo a Internet das coisas de uma maneira simples, válida e construtiva, ao mesmo tempo tentando minimizar a confusão de ideias sobre o tema.

1.3 OBJETIVOS ESPECÍFICOS

- Descrever as tecnologias, arquiteturas de redes e sistemas que suportam IoT;
- Entender os desafios da Internet das Coisas quanto à regulamentação e padronização;
- Descrever problemas e soluções na área de segurança de redes e IoT;
- Mostrar aplicações e benefícios da IoT em várias áreas do nosso cotidiano;
- Explanar sobre as expectativas de mercado e previsões até 2020.

1.4 METODOLOGIA DE PESQUISA

- Análise bibliográficas
- Traduções de obras com auxilio de ferramentas especificas
- Compreensão sobre o tema

1.5 DELIMITAÇÃO DO PROBLEMA

Existe uma confusão de ideias e sobreposição constante de termos relacionados, como “Internet of Everything", "Web of Things”, "Big Data", por exemplo e esta falta de consenso sobre o que é a “Internet of Things” e o que ela significa acaba por tornar um pouco difícil escrever um livro sobre o assunto.

1.6 ESTRUTURA DO TRABALHO

O presente trabalho será confeccionado em cinco capítulos sendo estes:

Capitulo 1 – Breve introdução incluindo apresentação dos objetivos, metodologia e delimitação do problema;

Capitulo 2 – Contendo referencial teórico sobre definição, arquitetura, tecnologias e interações tecnológicas;

Capitulo 3 – Sobre os desafios do IoT, envolvendo normas, protocolos e seguranças a serem aplicadas;

Capitulo 4 – Sobre aplicações de IoT, na indústria, na medicina, em casa, abrangendo a comunicação Maquina a Maquina (M2M, do inglês Machine to Machine) e a Identificação por Radiofrequência (RFID, do inglês Radio Frequency IDentification).

Capitulo 5 – Conclusão e considerações finais.

2 DEFINIÇÃO DE INTERNET DAS COISAS

De acordo com Peter Waher (2015) a Internet das Coisas é algo que obtemos quando conectamos as coisas, não operadas por seres humanos, à Internet. Atualmente a principal forma de comunicação da Internet é humana e segundo o autor a IoT pode ser considerada como a futura avaliação da Internet que realiza aprendizagem máquina a máquina (M2M, do inglês Machine to Machine) fornecendo conectividade para todos e tudo. (Peter Waher, 2015).

A União Internacional de Telecomunicações (ITU, do inglês International Telecommunication Union) define a IoT como *"Uma infraestrutura global para a sociedade da informação, permitindo serviços avançados através da interconexão (física e virtual) de coisas baseadas em tecnologias interoperáveis de informação e comunicação, existentes e em evolução* ". (ITU, 2012).

É definida também por Buckley como uma evolução radical da Internet atual em uma rede de objetos interconectados uma vez que não só colhe informações do ambiente e interage com o mundo físico, mas também usa os padrões existentes da Internet para fornecer serviços de transferência de informações, de análise, aplicações e comunicações. (Buckley, 2006).

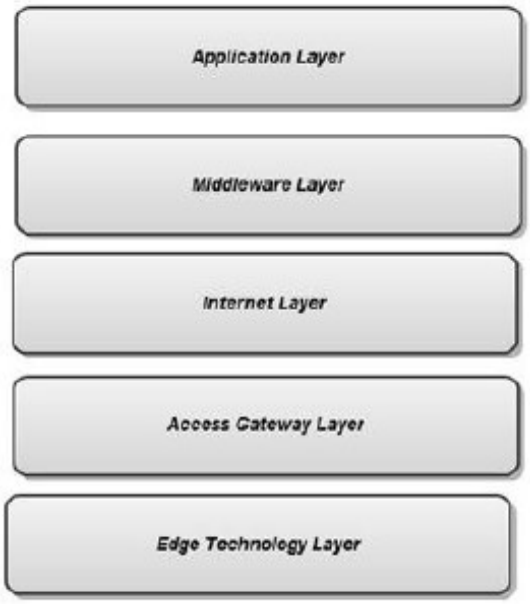
A ideia básica do IoT será permitir uma conexão autônoma e segura e troca de dados entre dispositivos e aplicações do mundo real (Fan e Chen, 2010) onde o IoT vai incorporar alguma inteligência em objetos conectados à Internet para se comunicar, trocar informações, tomar decisões, invocar ações. Tende assim fornecer serviços surpreendentes que o torna em crescente popularidade para as instituições acadêmicas, indústrias, bem como governos uma vez que tem o potencial de trazer significativos benefícios pessoais, profissionais e econômicos.

2.1 ARQUITETURA DA INTERNET DAS COISAS

Zarghami defendeu em sua tese uma arquitetura genérica em camadas projetada para responder às demandas de várias indústrias, empresas e sociedade para IoT. Esta arquitetura era constituída basicamente em cinco camadas (Fig. 1) contendo uma camada Edge Technology ou tecnologia da ponta que consiste no hardware que compõe sistemas incorporados, tags RFID, redes de sensores e todos os outros sensores em diferentes formas e que pode executar várias funções, como a coleta de informações de um sistema ou um ambiente, processamento de informações e suporte de comunicação. Uma camada Gateway ou caminho

de acesso que visa o tratamento de dados e será responsável por publicar e subscrever os serviços que são fornecidos pelos objetos conectados, encaminhamentos de mensagens e agilizar a comunicação entre plataformas. Uma camada Middleware ou intermediária que terá algumas funcionalidades críticas, como a agregação e filtragem dos dados recebidos dos dispositivos de hardware, realizando a descoberta de informações e fornecendo controle de acesso aos dispositivos para aplicativos. E uma camada Application ou de aplicação responsável pela entrega de vários serviços de aplicativos. Serviços esses que são fornecidos através da camada intermediária para diferentes aplicativos e usuários em sistemas baseados em IoT e podem ser usados em diferentes meios tais como indústrias, logística, varejo, saúde, etc. (Zarghami, 2013).

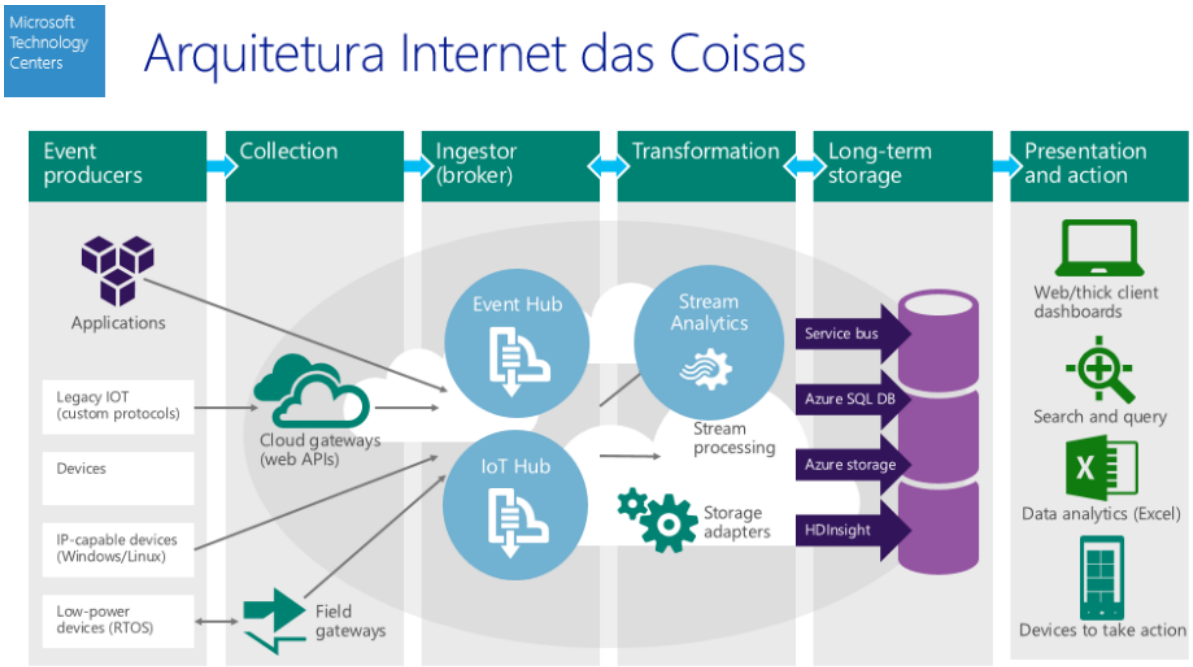
Figura 1 – Arquitetura genérica de IoT proposta por Zarghami



Fonte: Tese final de Zarghami, 2013.

No entanto sistemas ou soluções IoT possuem componentes de diferentes tecnologias que são gerenciados e controlados de forma independente, tendo em alguns casos camadas nas quais há interações com pessoas e não só técnicas entre componentes. (Sommerville, 2012). E para alguns foram criados modelos ou arquiteturas exclusivas (Fig. 2) que na verdade representam interpretações do conhecimento que estão presentes no contexto do sistema.

Figura 2 – Arquitetura de sistema de nuvem para IoT



Fonte: Divulgação Microsoft.

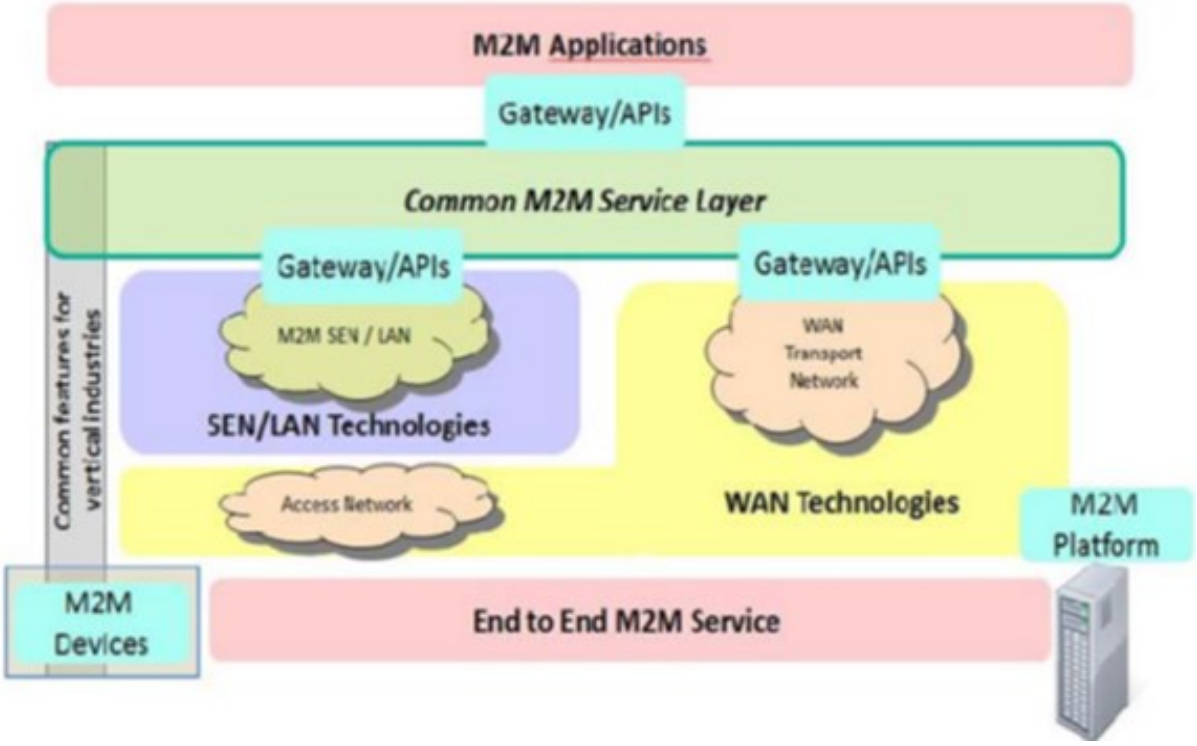
O fato é que uma arquitetura universal da IoT ainda não está definida, uma vez que o cenário atual de IoT é caracterizado pela presença de aplicativos construídos especificamente que operam em uma arquitetura de rede projetada, quase que exclusivamente, para a aplicação e a medida que os sistemas de IoT progridem. Eles precisarão se integrar com outros sistemas, e este é o lugar onde os principais desafios permanecem atualmente, pois muitas dessas aplicações operam em silos e têm uma arquitetura distinta que não se presta a interoperabilidade. (Pesquisa de mercados da Deutsche Bank, 2014).

Qualquer arquitetura geral que tenha sido seguida nos estágios iniciais da pesquisa de IoT precisará ser investigada e alterada pois a maioria das obras relacionadas à arquitetura IoT partiram do princípio de redes de sensores sem fio, porém no futuro um grande número de diferentes meios serão utilizados para permitir a comunicação entre dispositivos heterogêneos. (Castellani, 2010).

Para se atingir então o nível de integração que a IoT irar demandar, será necessária primeiro uma base comum para construir sub-arquiteturas, ou seja, um conjunto comum de blocos de construção, para o desenvolvimento da arquitetura do sistema que garantirá interoperabilidade em vários níveis. (Pesquisa de mercados da Deutsche Bank, 2014). Tendo em vista a importância do que está em jogo várias organizações de desenvolvimento de padrões (SDO, do inglês Standards Development Organizations), envolvidas no desenvolvimento da arquitetura de referência para o IoT e que publicam padrões de telecomunicações, se uniram

para formar uma arquitetura genérica oneM2M (Fig. 3) com o principal objetivo de desenvolver especificações para garantir a funcionalidade global dos sistemas e minimizar a fragmentação das arquiteturas M2M e IoT (oneM2M, 2013).

Figura 3 – Arquitetura básica oneM2M

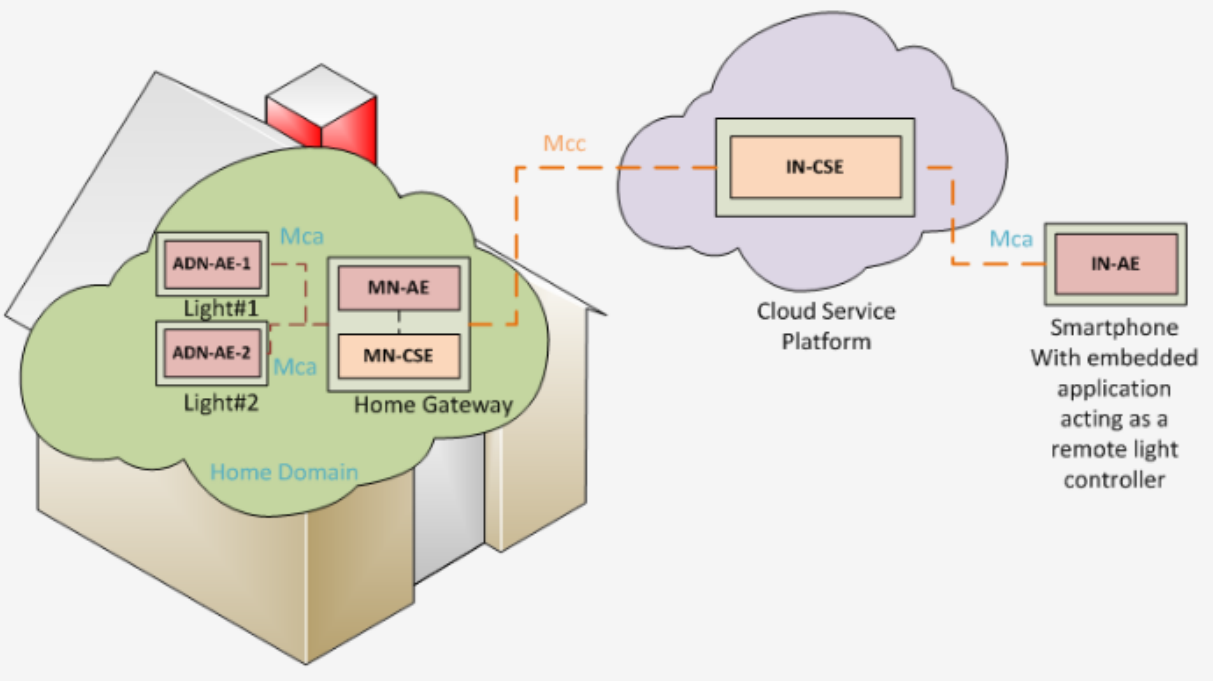


Fonte: oneM2M (http://onem2m.org).

Nesta arquitetura básica são apresentados três tipos de camadas sendo a M2M Application que é uma camada de aplicação, a Common M2M Service Layer que é uma camada de serviços comuns e End to End M2M Service que é a camada de serviços de rede. Na camada aplicação enquadra-se elementos de ponta, sensores, geolocalizadores, smartphone, que formam a chamada Entidade de Aplicação (AE, do inglês Application Entity) uma entidade que implementa uma ou mais lógicas de serviços identificados com uma AE-ID exclusiva, permitindo que uma solicitação de uma lógica de serviço faça uso do aplicativo desenvolvido para comunicar-se. Na camada de serviços comuns uma segunda entidade importante chamada Entidade de Serviços Comuns (CSE, do inglês Common Services Entity) representa uma solicitação de um conjunto de funções comuns que usam em uma arquitetura funcional (Fig. 4) pontos de comunicação denominados Mca (uma abreviação mnemônica do inglês M2M communications Application Entity), aplicada quando a interação é entre a AE e CSE, e ponto de comunicação Mcc (outra abreviação mnemônica do inglês M2M communications Common

Services Entity), usado para acessar as entidades de serviço de rede subjacentes identificados com uma CSE-ID exclusiva, que pode ser um ponto de conexão de infraestrutura de serviços comuns (IN-CSE, do inglês Infrastructure Node Common Services Entity) a um gateway doméstico de serviços comuns (MN-CSE, do inglês Middle Node Common Services Entity). Este conjunto permitiria, por exemplo, um aplicativo de smartphone desenvolvido com recursos para interagir diretamente com a plataforma de serviço da nuvem, controlar remotamente as luzes do ambiente da casa (oneM2M, 2013). As especificações desenvolvidas pela oneM2M serviram como um projeto estrutural comum para redes e sistemas para executar um amplo conjunto de aplicações e pretendiam desenvolver uma camada de serviço comum que facilitasse a interoperabilidade entre redes de sensores, dispositivos e aplicativos baseados em nuvem.

Figura 4 – Arquitetura funcional oneM2M

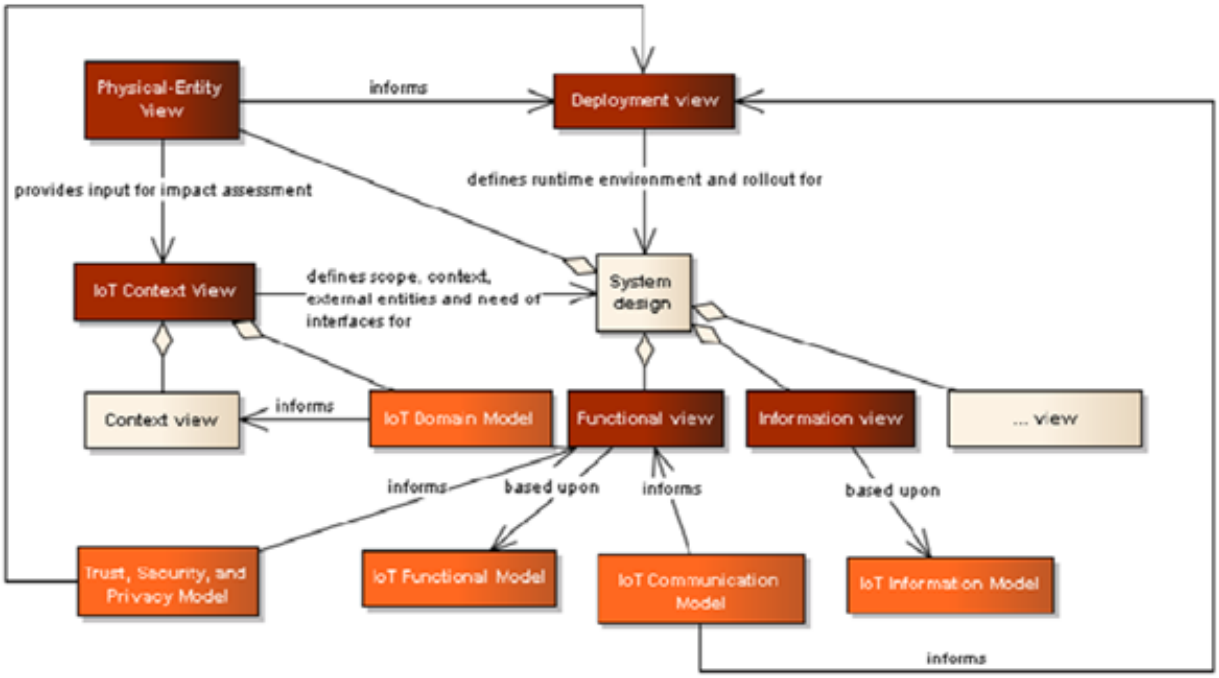


Fonte: oneM2M (http://onem2m.org).

Paralelamente à oneM2M, a comissão europeia estabeleceu o IoT-A (do inglês Internet of Thing Architecture), que criou o Modelo de Referência de Arquitetura (ARM, do inglês Architecture Reference Model) e definiu os principais blocos de construção de quase todos os sistemas IoT. A IoT-A é uma fundação da comissão europeia na qual as empresas de software podem capitalizar sobre os benefícios do desenvolvimento de plataformas orientadas para o consumidor, incluindo hardware, software e serviços, e em seu projeto denominado "European Lighthouse Integrated Project" afirma que abordou durante três anos a arquitetura

do IoT e criou o modelo de referência arquitetônico proposto, juntamente com a definição de um conjunto inicial de blocos de construção (Fig. 5), os quais são referidos como visões de arquitetura: Visão física, Visão de contexto, Visão funcional, Visão de informação e Visão de implementação. (IoT-A, 2013). Esse modelo de referência foca conjuntos de mecanismos abstratos ao invés de arquiteturas de aplicativos concretas.

Figura 5 – Arquitetura proposta pela IoT-A



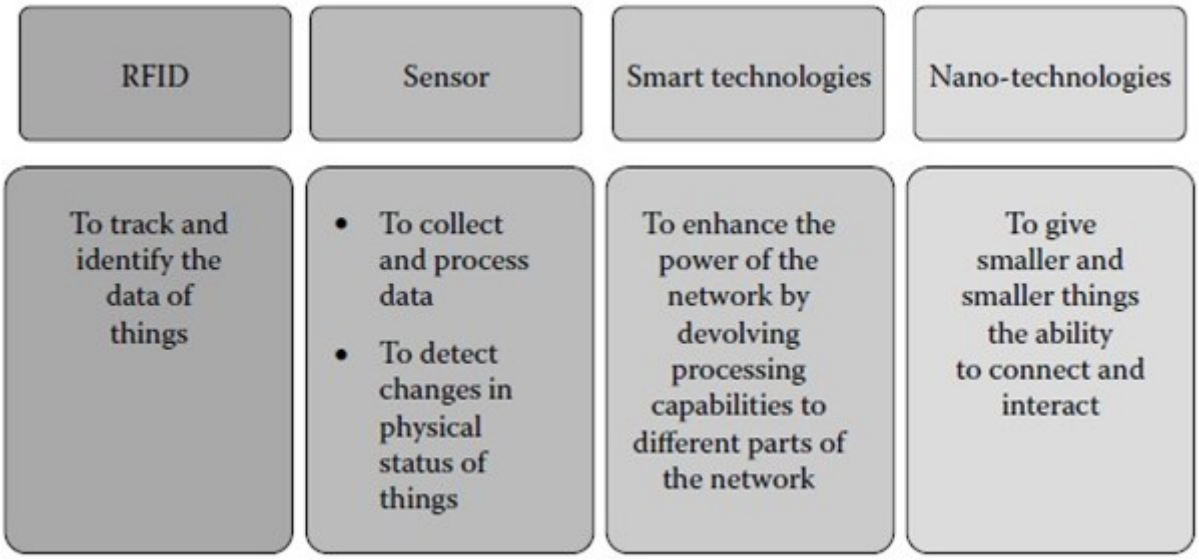
Fonte: IoT-A, European Commission (http://iot-a.eu).

De acordo com Deutsche Bank o modelo de referência de arquitetura proposto pelo IoT-A é o que mais se destaca e fornece um conjunto de abstrações para desenvolver arquiteturas concretas podendo ser usado em numa grande variedade de casos de uso de IoT. Mas ainda assim, infelizmente, um único sistema de rede para o IoT não pode ser estabelecido usando apenas as visões acima, dada a vasta gama de casos de uso, dada a diferenças nos dispositivos físicos e às várias maneiras que esses elementos serão conectados por Wi-Fi, rádio celular, Bluetooth, além de uma série de canais de comunicação, tornando quase impraticável ter hoje uma solução universal para todos os cenários em que as aplicações IoT são susceptíveis de serem implantadas. (Pesquisa encomendada Deutsche Bank, 2014).

2.2 ELEMENTOS

A implementação do IoT ainda será constituída por redes heterogêneas e amplamente distribuídas onde a identificação por radiofrequência, sensores, tecnologias inteligentes e nanotecnologias são os principais contribuintes para uma variedade de serviços (Fig. 6). Essa rede abrange uma infraestrutura global, incluindo software, hardware e serviços, que serão utilizados para suportar essas redes de informação. As coisas físicas integradas poderão trocar dados sobre as propriedades físicas e informações que elas percebem em seu entorno (Peter Waher, 2015).

Figura 6 – IoT tecnologias subjacentes

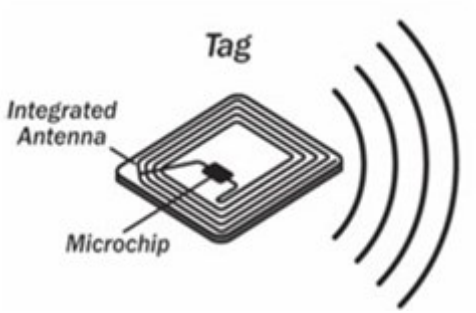


Fonte: Learning Internet of Things.

Para identificar dispositivos, poderão ser utilizadas tecnologias de identificação, como, por exemplo, RFID, que permitem que cada dispositivo seja identificado de forma exclusiva. O RFID é um método para identificação automática e captura de dados (AIDC, do inglês Automatic Identification and Data Capture) que utiliza campos eletromagnéticos para identificar e rastrear automaticamente etiquetas anexadas aos objetos (Fig .7) compostas por um chipset, que armazena os dados exclusivos e os recursos de segurança disponíveis, e por uma antena que permite que o chip receba energia e transmita informações. Essas tags contêm informações armazenadas eletronicamente e não precisam estar diretamente na linha de visão do leitor e podem ser separadas em tags passivas, que coletam energia a partir das ondas de rádio de interrogação de um leitor RFID próximo, e em tags ativas, que possuem uma fonte de

energia local como uma bateria e podem operar a centenas de metros do leitor de RFID (Wayback Machine, 2016).

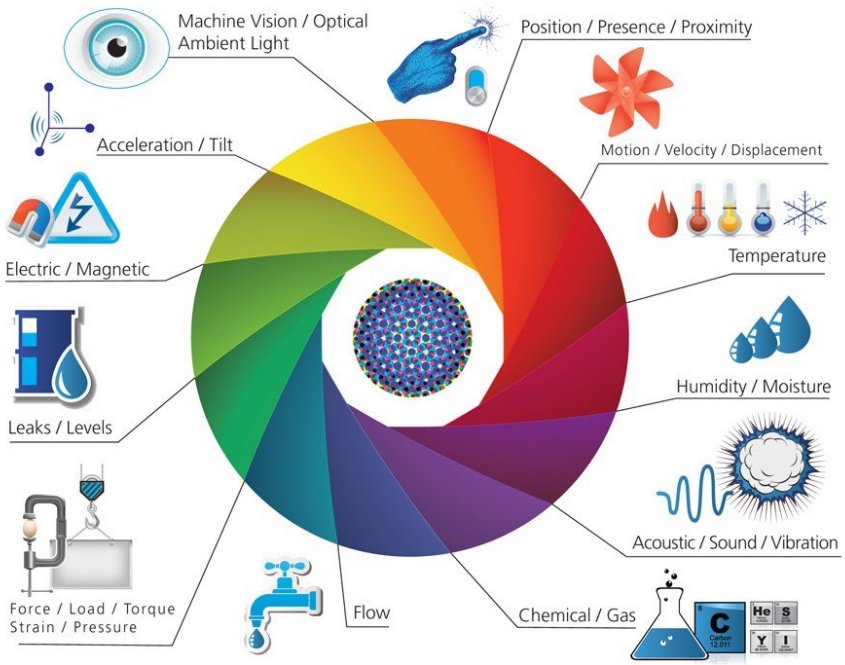
Figura 7 – Etiqueta RFID



Fonte: InTechOpen (https://intechweb.wordpress.com/).

Sensores e atuadores, segundo empresa de pesquisa Harbor, são os elementos chave para a coleta e saída de dados valiosos e serão os grandes responsáveis por permitir que os dispositivos conectados se comportem de forma autônoma. Atualmente uma gama de sensores e atuadores é usada para tornar isso realidade (Fig. 8), conscientizando o ambiente em termos de contexto e assim capazes de tomar suas próprias decisões inteligentes (Harbor Research, 2017).

Figura 8 – Infográfico da Harbor Sensores



Fonte: IoT Infographic Overview Postscapes (http://postscapes.com).

A biometria já está integrada nos telefones móveis inteligentes e espera-se que seja usada em conjunto com circuitos de TV em locais altamente sensíveis ao redor da cidade. Os cartões de identificação nacionais também se tornarão uma ferramenta essencial para a identificação de um indivíduo. Além disso, as cidades inteligentes em 2020 exigirão sistemas de segurança de identificação automática em tempo real (Vermesan e Friess, 2014).

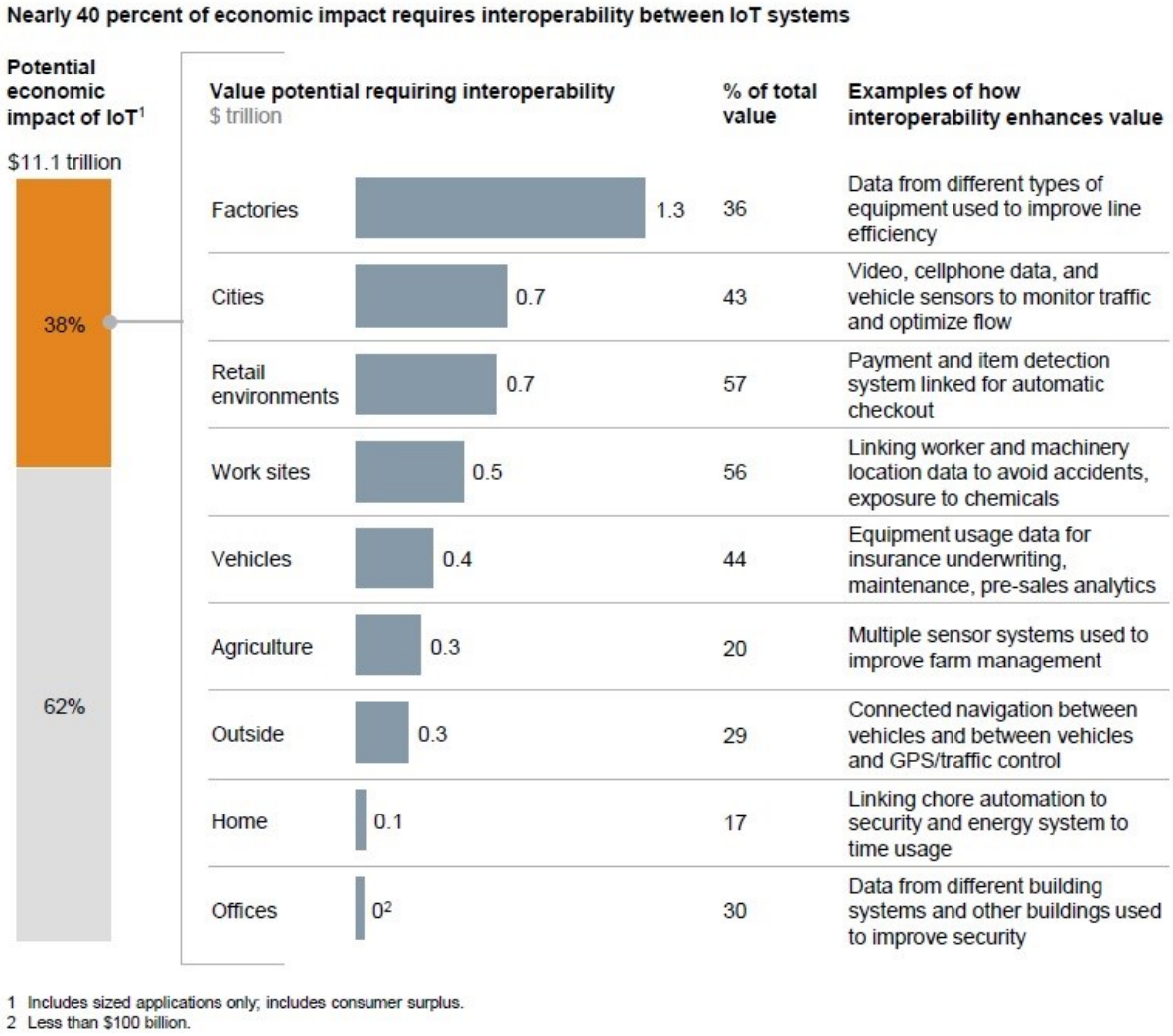
2.3 INTERAÇÕES TECNOLÓGICAS

Assim como na Internet uma única entidade não pode assumir a responsabilidade por tudo, o seu funcionamento não depende de uma série de serviços isolados, mas da capacidade de coexistir, intercambiar dados e interagir com os usuários. Esta capacidade é a interação tecnológica e será importante para o desenvolvimento da IoT que baseia-se na interação e cooperação entre os serviços e seus usuários (Peter Waher, 2015).

A interação tecnológica será um ponto chave para analisar as aplicações da Internet das Coisas no contexto das configurações dos ambientes físicos em que esses sistemas são implantados, como casas, escritórios e fábricas. Essa importante característica é necessária para tornar as aplicações IoT interoperáveis entre si, fazendo os sistemas IoT se comunicarem uns com os outros como ligar o monitor de saúde na residência de um paciente ao sistema de informática de saúde do hospital por exemplo. Isto implica em um desafio complexo de projeto de sistemas que requer coordenação em vários níveis (tecnologia, ciclos de investimento, mudança organizacional, etc.). (Daniel Camara e Navid Nikaein, 2016). Essa interação poderá ser realizada pela adoção de padrões abertos ou pode ser alcançada através da implementação de sistemas ou plataformas que permitem que diferentes sistemas IoT se comuniquem entre si possibilitando comunicação de dispositivos que usam protocolos distintos. (Peter Waher, 2015).

Pesquisas como do instituto McKinsey apontam que esta característica será a chave da análise dos benefícios aplicações IoT sendo responsável por cerca de 40% (Gráf. 1) do valor potencial que pode ser gerado uma vez que reflete a capacidade dos dispositivos e sistemas IoT trabalharem em conjunto (James Manyika et al, 2015).

Gráfico 1 - Análise do McKinsey Global Institute



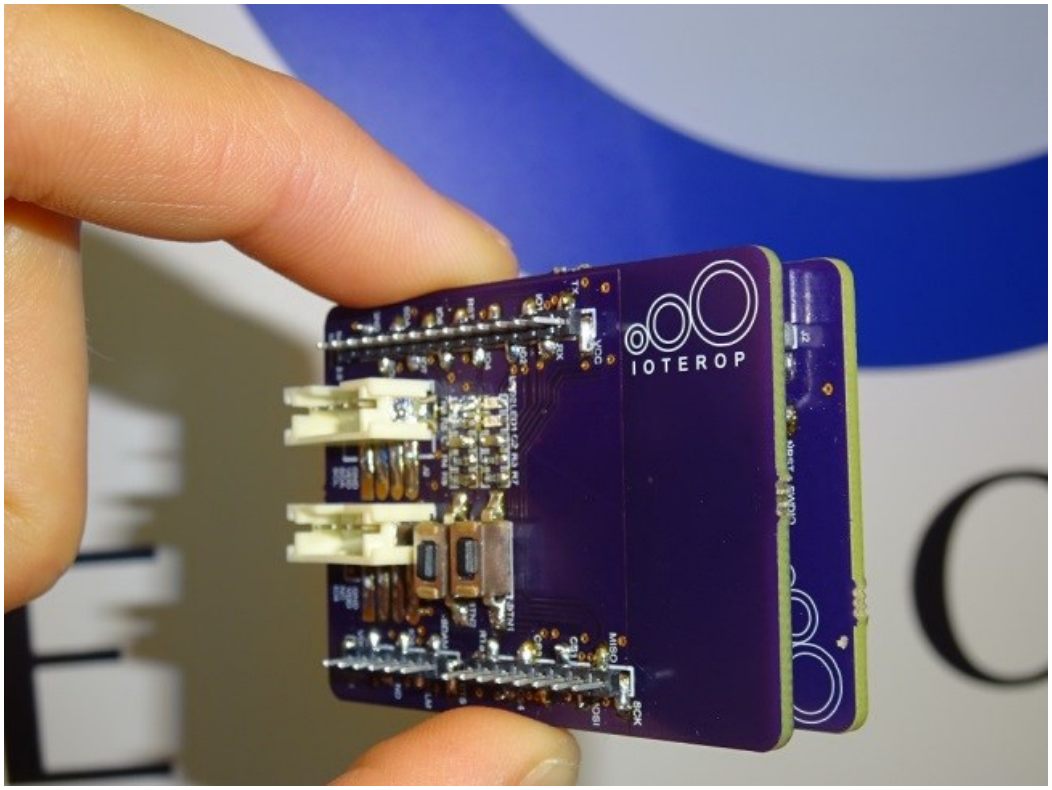
Fonte: Entrevistas de especialistas instituto McKinsey

A interação tecnologia é sem dúvida um dos grandes próximos passos do IoT que vai permitir, à sua maneira, a criação de serviços e aplicações abertas e interoperáveis de valor agregado, viabilizadas pela sua interligação, de forma a poderem ser integradas nos atuais e novos processos de negócio e desenvolvimento. Tendo por principal preocupação a garantia vital que os componentes da rede irão interoperar para liberar todo o valor do IoT e evitar a indisponibilidade de alguns serviços para usuários finais. (Vermesan e Friess, 2014).

Muitas fontes e empresas estão apontando as dificuldades da interação tecnológica e enfatizam a necessidade urgente de vencer este desafio do IoT, mas algumas estão propondo soluções para este desafio e entre elas a IoTerop, fundada na França por especialistas em tecnologia de gerenciamento de dispositivos que visam, através de um esforço coletivo, trazer um conjunto comum de padrões para bilhões de objetos conectados nos próximos anos. Reúne as com as principais empresas de alta tecnologia como Palm, ACCESS, Intel e grandes players

do setor como Microsoft, Qualcomm, ARM. Estes especialistas estão desenvolvendo um produto chamado sensorHub (Fig. 9), um dispositivo eletrônico inteligente que foi desenvolvido para a indústria com objetivo de facilitar a interoperabilidade de seus objetos conectados, bastando apenas conectar seus sensores no sensorHub que visa fornecer conexões protegidas com autenticação e criptografia. (IoteropCompany, 2017)

Figura 9 – SensorHub da IoTerop



Fonte: http://ioterop.com/sensorhub/

O sensorHub é incorporado com atualização de Firmware além de possui recursos de gerenciamento de dispositivos usando o protocolo LwM2M, abreviação do inglês Lightweight M2M, que é um protocolo de gerenciamento de dispositivos projetado para redes de sensores buscando ser um padrão comum para gerenciar dispositivos leves e de baixa potência (OMA, 2014). Ele está comercialmente disponível a partir do dia 28 de agosto de 2017 e seu público alvo são os grupos que utilizam o protocolo LwM2M, entre eles grandes empresas como a AVSystem, Ericsson, Gemalto, Huawei, Nokia, Sierra Wireless, que vem adotando o LwM2M por ser um modelo baseado em REST construído no padrão do protocolo CoAP (Constrained Application Protocol) que apresento na seção 3.2 protocolos.

3 DESAFIOS DA INTERNET DAS COISAS

Entre as principais dificuldades e desafios do IoT nos próximos anos estão a regulamentação, padronização de protocolos e garantia de segurança. A exemplo do protocolo ainda não foi definido um padrão para todas as aplicações, pois cada um tende a ser eficiente para apenas um único problema. Existem hoje um bom número de protocolos de rede para IoT aplicáveis nos pequenos dispositivos como HTTP, MQTT, CoAP, UPnP, XMPP, etc., mas cada qual com uma tecnologia de aplicabilidade restrita. (Woodside Capital Partners, 2015).

Muito em breve o IoT será incorporado em quase todos dispositivos móveis, medidores de estacionamento, termostatos, monitores cardíacos, pneus, estradas, prateleiras de supermercados e uma quantidade tão grande de dispositivos conectados com IoT será igualmente propensa a uma enorme exploração de vulnerabilidades, problemas de privacidade e segurança. Para isso precisamos de regulamentos adequados e organizados tanto para evitar tais riscos de segurança como para lidar com os riscos de todos os dispositivos IoT conectados (Peter Buttler, 2017).

3.1 REGULATÓRIO

Embora existam hoje certos padrões como o CIP (Critical Infrastructure Protection) pela NERC (North American Electric Reliability Corporation's) estabelecendo a segurança cibernética para minimizar as ameaças potenciais e proteger os dados on-line de infraestruturas críticas, um regulatório especifico e voltado para atender o IoT ainda não esta definido, nem mesmo quem será o responsável por sua regulamentação. É uma tarefa complicada determinar quem possa regular com eficácia a internet das coisas. O único consentimento geral em que algumas uniões chegaram é que tais regulamentos, se adotados pelos advogados e órgãos reguladores, poderiam tornar qualquer projeto de IoT operacionalmente ou financeiramente inviável (Bruce Schneier, 2016).

Recentemente a União Européia iniciou um processo de revisão de seu regulamento de privacidade eletrônico denominado ePrivacy Regulation, que complementa o regulamento europeu de proteção de dados (EDPR, do inglês, European Data Protection Regulation) responsável por regular o processamento de dados pessoais em comunicações eletrônicas. Assim que sua proposta foi publicada algumas reclamações já foram declaradas desde à redações do projeto não serem totalmente claras como a interpretação mais literal de algumas disposições, até a questionamentos mais específicos como as regras sobre a portabilidade dos

dados gerados pelos dispositivos de IoT. Assim frente a grande quantidade de questões abertas, a União Européia lançou uma consulta pública sobre o tema no inicio deste ano destinada a identificar e abordar questões que possam ter impactos relevantes no futuro das empresas que investem na Europa (Giulio Coraggio, 2017).

No Brasil uma consulta pública também foi realizada no inicio do ano pelo MCTIC (Ministério da Ciência, Tecnologia, Comunicações e Inovações) denominado Plano Nacional de Internet das Coisas. Porem logo em seguida a Anatel, Agência Nacional de Telecomunicações, através de seu gerente de regulação Nilo Pasquali, informou que não vai criar um marco regulatório para Internet das Coisas descartando assim a criação de regulamento específico. Em debate sobre os desafios jurídicos para o desenvolvimento da IoT no Brasil justificou que o objetivo é desenvolver a Internet das Coisas sem criar dificuldades e possibilitar inovação (Portal Computerworld, 2017).

A comissão federal de comércio dos Estados Unidos também descartou a criação de um regulamento para IoT no início deste ano informando, através de seu chefe interino, Maureen Ohlhausen, que a comissão não vai impor regulamentos obrigatórios aos dispositivos de IoT e que não irão intervir até que haja algum evento que venha a prejudicar os consumidores (Gareth Corfield, 2017).

3.2 PROTOCOLOS

O HTTP (Hypertext Transfer Protocol), um dos mais conhecidos, que é um protocolo utilizado principalmente para navegar entre as páginas usando um navegador que se comunica com o servidor, é hoje usado também em comunicação máquina a máquina (M2M), automação e Internet das Coisas, entre outras coisas por ser facilmente acessível e fácil de se relacionar. Basicamente HTTP é um protocolo de solicitação e resposta sem estado onde os clientes solicitam informações de um servidor e o servidor responde a essas solicitações de acordo. O pedido é composto de um método, um recurso, alguns cabeçalhos e algum conteúdo opcional. A resposta é composta de um código de status de três dígitos, alguns cabeçalhos e algum conteúdo opcional. Essa comunicação entre o cliente e o servidor em HTTP é feita através de uma conexão TCP (Transmission Control Protocol) que garante que os pacotes não são perdidos e são recebidos na mesma ordem em que foram enviados e hoje funciona em cima do Internet Protocol (IP), protocolo onde as máquinas são endereçadas usando um endereço IP e se comunicam entre diferentes redes de área local e que podem usar diferentes esquemas de endereçamento, entre os mais comuns o MAC (media access control), um endereço de controle

de acesso à mídia utilizado em redes de tipo Ethernet. (Kurose e Ross, 2016). Normalmente HTTP pode ser utilizado para adicionar suporte web aos sensores de IoT para que possam publicar seus dados e informações em um servidor na Internet. Este servidor por sua vez poderá até atuar como um corretor e informar as partes interessadas sobre os valores dos sensores. Nesta situação HTTP se torna um protocolo que simplifica a manipulação de eventos, porem o torna difícil para obter valores momentâneos devido a necessidade de declaração de bloqueio, sincronização, etc, a fim de garantir que o acesso aos valores momentâneos só esteja disponível de um segmento de cada vez, o que reforça que não existe um único protocolo perfeito, cada protocolo terá seus pontos fortes e suas fraquezas (Peter Waher, 2015).

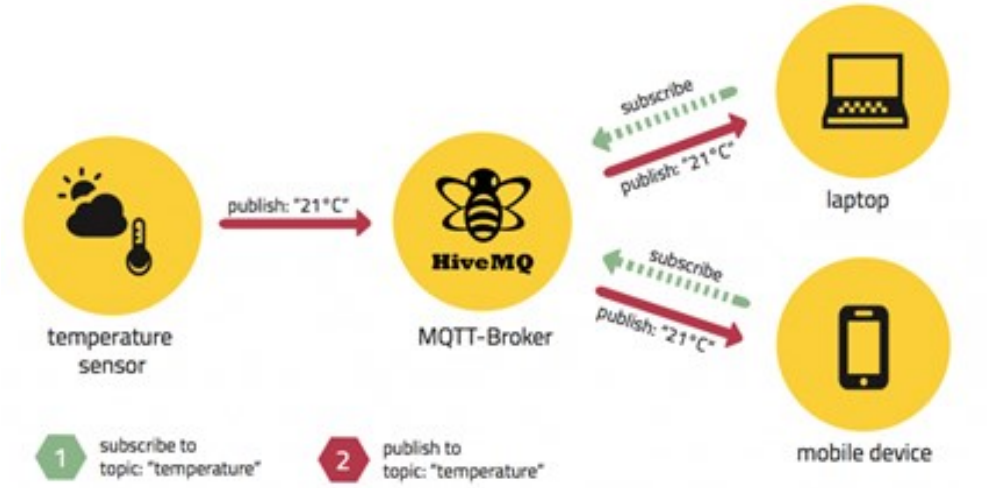
O UPnP (Universal Plug and Play), usado por quase todos os produtos de eletrônicos de consumo ativados pela rede usados em sua casa ou escritório, é um protocolo ou uma arquitetura que usa vários protocolos e baseia-se principalmente em uma aplicação HTTP em que clientes e servidores são participantes. Ele utiliza o SSDP (Simple Service Discovery Protocol), um protocolo para a descoberta de dispositivos na rede, e o GENA (General Event Notification Architecture), um protocolo para subscrições de eventos e notificações. Ambos são baseados em HTTP e introduzem novos métodos para pesquisar, notificar e assinar e cancelar a inscrição de um evento sendo estendido para que ele possa ser usado sobre TCP, bem como UDP onde ambos usam endereçamento unicast (HTTPU) e endereçamento multicast (HTTPMU) (Universal Plug and Play Forum, 1999). Ele poderia a exemplo de Peter Waher ao ser estendido com HTTP, utilizado como um meio de fornecer descoberta automática de dispositivo de IoT e um método alternativo para notificação de eventos além de detectar alterações nos estados dos dispositivos. Basicamente com o UPnP traria benefícios em simplificar o HTTP e usá-lo sobre o UDP em vez do TCP. Outro ponto forte do UPnP é a sua interação com a manipulação disponível da biblioteca de serviços documentada e como esses documentos podem ser usados para desenvolver soluções onde os dispositivos possam vir a ser substituíveis (Peter Waher, 2015).

O CoAP (Constrained Application Protocol) é um protocolo de aplicação restrita projetado para traduzir facilmente o HTTP para uma integração simplificada com a web e que pode ser executado na maioria dos dispositivos que suportam UDP ou um análogo UDP (Walter, 2011). Basicamente ele substitui os cabeçalhos de texto usados em HTTPU com cabeçalhos binários mais compactos e reduz o número de opções disponíveis no cabeçalho trazendo baixa sobrecarga e simplicidade que são extremamente importantes para dispositivos de IoT e M2M uma vez que estes tendem a ser profundamente incorporados e têm muito menos memória e fonte de alimentação do que os dispositivos tradicionais da Internet. Além disso, ele

também reduz o conjunto de métodos que podem ser usados permitindo que se tenham apenas quatro métodos: GET, POST, PUT e DELETE e suas chamadas de método podem ser feitas usando serviços de mensagens confirmáveis e não confirmáveis. O ponto forte do CoAP é que ele fornece um conjunto de extensões úteis, entre elas uma que fornece um algoritmo de transferência em bloco permitindo transferir grandes quantidades de dados. Atualmente o uso deste protocolo é o meio simples para criar aplicativos IoT e preferencialmente usado na maioria dos projetos de sensores, atuadores e controladores, porém não é tão eficiente em comunicação para publicação ou subscrição de mensagem (Peter Waher, 2015).

O MQTT (Message Queue Telemetry Transport) é um protocolo que usa agentes de mensagens (Fig. 10) baseando-se nos métodos PUBLISH-SUBSCRIBE, um padrão de mensagens publicadas em classes sem conhecimento de quais assinantes existem e estes por sua vez expressam interesse em uma ou mais classes e só recebem mensagens que lhes são de interesse sem conhecimento de quais editores existem, tendo três principais agentes: editores ou publish, com função de conectar-se ao corretor de mensagens e publicar conteúdo; assinantes ou subscribe, com função de se conectarem ao mesmo agente de mensagens e se inscreverem no conteúdo que eles estão interessados; e agente de mensagens ou message broker, que basicamente funciona como um servidor para retransmitir mensagens entre clientes garantindo que o conteúdo publicado é retransmitido para os assinantes interessados (HiveMQ, 2015).

Figura 10 – Arquitetura publish/subscribe MQTT



Fonte: HiveMQ enterprise MQTT Broker.

Para IoT o MQTT será principalmente utilizado como um message broker fora do firewall, uma vez que um dos principais problemas dos protocolos HTTP, UPnP e CoAP é justamente como cruzar os limites do firewall que bloqueiam as tentativas de conexão e

normalmente escondem uma rede doméstica ou empresarial por trás de um único endereço IP. Com ele na função de message broker será possível cruzar os limites de firewall uma vez que todos os pontos finais em uma conversa atuam como clientes para um agente de mensagens comum que fica fora do firewall e, portanto, acessível a todos objetos (Peter Waher, 2015). Este protocolo trabalha com três níveis de qualidade de serviço durante a publicação de conteúdo. Um nível mais baixo sem confirmação onde a mensagem é entregue no máximo uma vez para cada assinante sem reenvio. Um segundo nível que é um serviço com confirmação onde cada destinatário confirmar a recepção das informações publicadas e se não for recebida a confirmação as informações podem ser enviadas mais uma vez. E um terceiro nível chamado de serviço assegurado onde as informações são transmitida e entregue a cada passo com confirmações o que torna possível garantir que o conteúdo é entregue exatamente uma vez a cada assinante (MQTT community, 1999). O ponto fraco do protocolo MQTT é que ele fica limitado a um único padrão de comunicação publish-subscribe limitando as aplicações em que um objeto só publica dados para muitos consumidores de seus dados impossibilitando mensagens individualmente personalizadas, valores momentâneos, ou comunicação em tempo real ou mesmo bidirecional, além de ter um fraco suporte para a autenticação de usuário (Peter Waher, 2015).

O XMPP (Extensible Messaging and Presence Protocol) é um protocolo aberto padronizado pela IETF (Internet Engineering Task Force) que foi originalmente projetado para uso em aplicativos de mensagens instantâneas em tempo real onde mensagens menores são enviadas com a menor latência possível e sem qualquer persistência (XMPP community, 2002). Em aplicações de IoT o protocolo XMPP será muito bem vindo devido à sua flexibilidade e riqueza de padrões de comunicação. Ele também usa agentes de mensagens para ignorar barreiras de firewall assim como o MQTT porem além do método PUBLISH-SUBSCRIBER, ele suporta outros padrões de comunicação, como REQUEST-RESPONSE ponto a ponto, um padrão de troca de mensagens com solicitação e resposta a solicitação que permite que duas aplicações tenham uma conversação bidirecional entre si em um canal, e mensagens assíncronas padrões esses que vão permitir algumas facilidades como: associação global, onde os servidores criam conexões entre si de forma segura para trocar mensagens entre seus domínios; identidade global, onde os servidores fornecem a cada cliente uma identidade autenticada; detecção de presença, enviando uma assinatura que se aceito pelo cliente remoto trará mensagens sempre que o estado do contato for alterado informando se ele está on-line, off-line, ausente, ocupado; autorização, que vai assegurar aos dispositivos com capacidade de tomada de decisão limitada que somente a comunicação autorizada será retransmitida; e delegação de confiança, que acaba

sendo uma camada adicional de segurança a cada projeto de IoT, entre outras facilidades para que se tenha uma experiência de comunicação bem mais rica com o uso deste protocolo (Peter Waher, 2015).

3.3 SEGURANÇA

Muitas empresas têm experimentado desde a implantação nas primeiras gerações da Web o ataque de hackers para fins maliciosos e por isso devem se preocupar ao desenvolver um produto para uso em IoT, evitando que uma pessoa experiente possa assumir o controle de dispositivos vulneráveis conectado à Internet. Segundo Peter Waher existem muitas soluções e produtos comercializados hoje sob o rótulo IoT que não possuem arquiteturas básicas de segurança e isso não só deixa os dispositivos em casa sob risco, mas também deixa a automação de edifícios, carros, ônibus, aeroportos, serviços de saúde, aplicações de logística e de automação industrial vulneráveis a ataques (Peter Waher, 2015) e para tanto se torna necessário criar contramedidas para proteger suas soluções de IoT.

No entanto proteger a Internet das Coisas será uma tarefa complexa e difícil, sua população estimada em bilhões de objetos, que irão interagir uns com os outros e com outras entidades, como seres humanos ou entidades virtuais, criam muitas possibilidades de ataques disponíveis à pessoas mal-intencionadas ataque a vários canais de comunicações, ameaças físicas, negação de serviço, fabricação de identidade entre outras (Babar e Mahalle, 2010).

4 APLICAÇÃO DE IOT

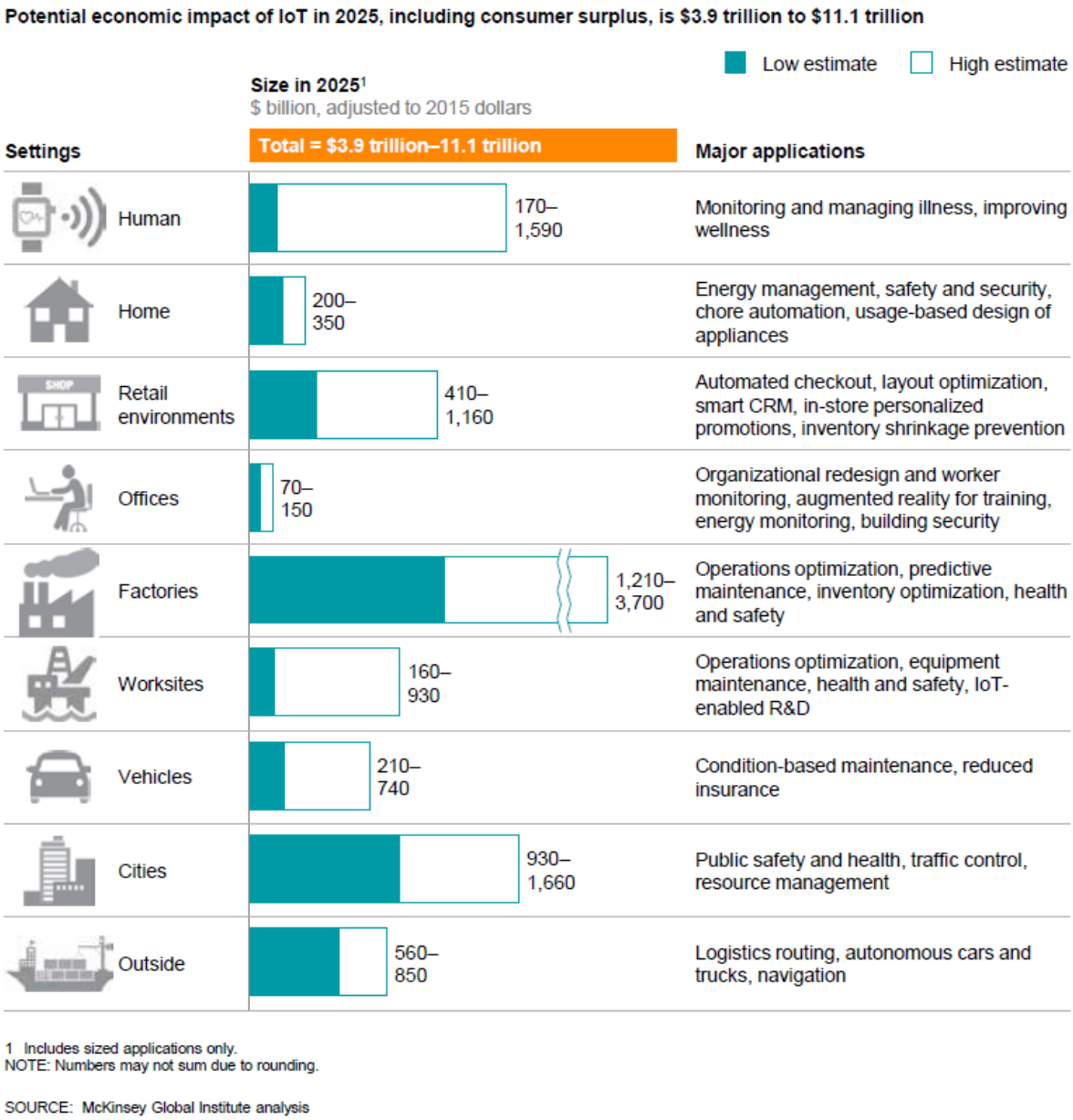
Em um futuro próximo, além do seu celular, muitos objetos estarão conectados à internet. Seu carro poderá ser monitorado em tempo real e avisar na tela do seu celular as necessidades de manutenção, aumentando assim os níveis de segurança. A sua geladeira poderá enviar uma lista de compras para o supermercado, que entregará os produtos na sua casa. O IoT recebeu uma atenção considerável e crescente nos últimos anos devido ao seu potencial para mudar radicalmente a nossa vida diária. São inúmeras as possibilidades da Internet das Coisas (Fig. 11) que conectará milhões de objetos do nosso dia a dia à internet. (Nokia Networks, 2016).

Figura 11 – Alguns domínios de aplicações de IoT

Fonte: Oi SA e Nokia Networks (2016).

São muitos os domínios de aplicações que serão impactados pelo IoT que podem ser classificadas com base no tipo de disponibilidade de rede, cobertura, heterogeneidade, escala e envolvimento do usuário. Não há quase nenhuma área de aplicação onde o IoT não consiga encontrar uma função e principalmente não há área de aplicação onde a IoT não traga alguma vantagem econômica ao longo do tempo (Gluhak, 2011). O McKinsey Global Institute em suas pesquisas, em especial a "Mapeando o Valor Além do Ciclo de Hype", estimou que o valor potencial total para as aplicações que abrangeram em nove áreas será de 3,9 a 11,1 trilhões de dólares por ano (Gráf. 2) em 2025 (McKinsey & Company, 2015).

Gráfico 2 - Potencial econômico de aplicações de IoT



Fonte: Mapping the value beyond the hype, McKinsey Global Institute, 2015

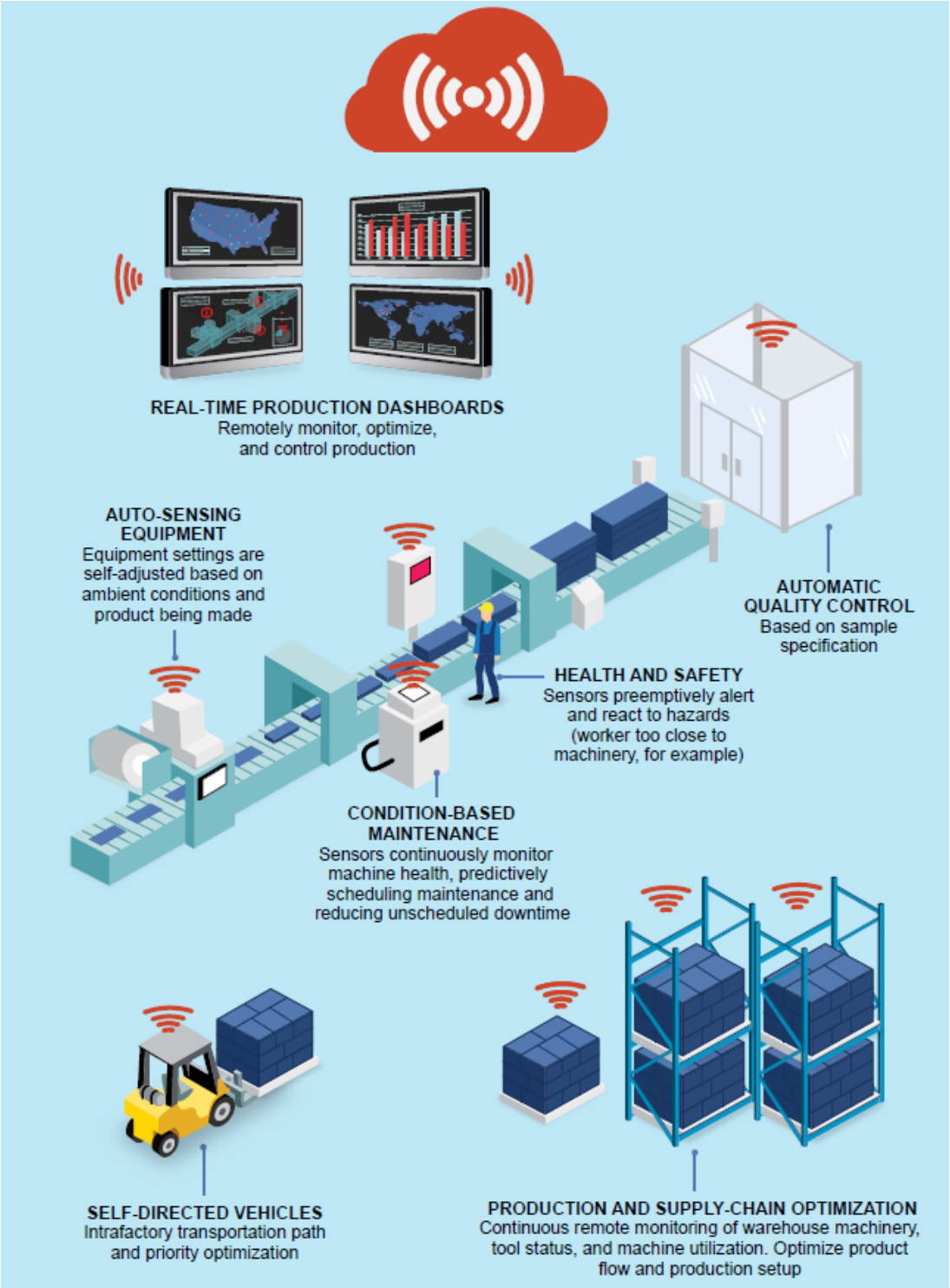
O maior ganho para valor potencial criado pelas aplicações IoT em 2025 será para domínio de aplicações industriais, que incluem fabricas, hospitais e fazendas com valor de até 3,7 trilhões de dólares por ano em 2025, praticamente um terço de todo o valor econômico potencial que estimaram. O segundo maior ganho está no domínio da aplicação em cidades com valor de até 1,7 trilhões de dólares por ano, seguido por saúde humana, com um valor potencial de até 1,6 trilhões de dólares por ano (McKinsey & Company, 2015).

4.1 APLICAÇÕES INDUSTRIAIS

A Internet das Coisas já está desempenhando um papel crítico na próxima fase de automação de indústrias com a digitalização completa dos processos de produção, unindo os mundos digital e físico dentro das fábricas e indústrias. Um dos principais aspectos é a capacidade de monitorar e controlar todas as ferramentas de produção além de usar os dados coletados para melhorar a produtividade e a qualidade. Isso coloca a tecnologia IoT no coração de uma nova onda de inovação que, como na primeira e segunda revoluções industriais, deverá gerar melhorias na produtividade (McKinsey & Company, 2015).

A aplicação de maior potencial será na otimização de operações tornando os vários processos dentro da fábrica mais eficientes. Isso inclui o uso de sensores, ao invés do julgamento humano, para ajustar o desempenho das maquinas e de certa forma manter livre de erro humano. Também envolve o uso de dados das máquinas de produção para ajustar os fluxos de trabalho que poderá ser feito por mecanismos de rastreamento, monitoramento e ajuste remoto, com base em dados de sensores de diferentes partes da planta de uma indústria. Outras aplicações também valiosas do IoT para indústrias serão a manutenção preditiva e otimização de inventário. A manutenção preditiva envolve o uso de sensores para monitorar as máquinas de forma contínua para evitar avarias e determinar quando a manutenção será necessária, em vez de depender de rotinas de manutenção agendadas regularmente e o gerenciamento de inventário pode melhorar reabastecendo automaticamente as caixas de peças com base nos dados de peso ou altura gravados pelos sensores, estas são apenas amostras (Fig. 12) das muitas possibilidades e principalmente do potencial econômico que IoT pode agregar (James Manyika et al., 2015).

Figura 12 – Amostra de algumas aplicações de IoT na indústria

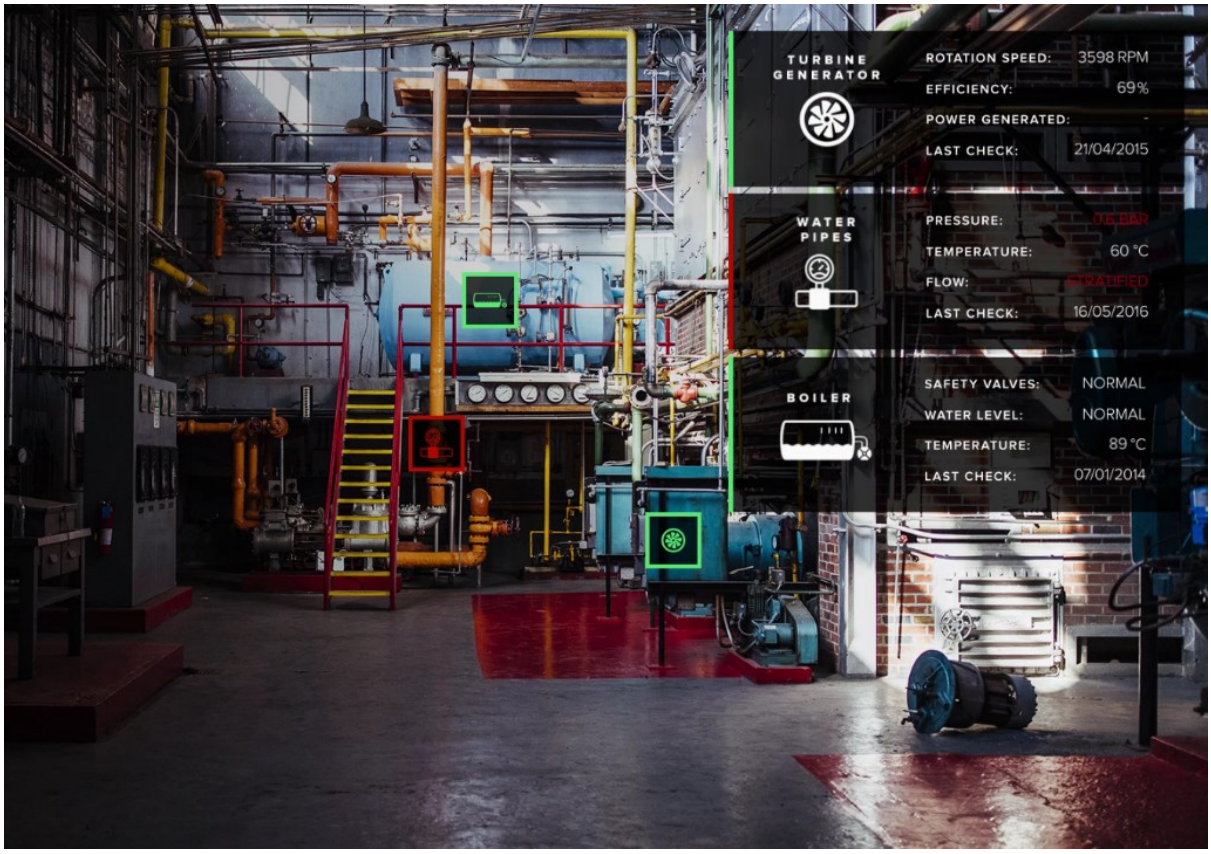


Fonte: Mapping the value beyond the hype, McKinsey Global Institute, 2015.

Para que essas e outras aplicações IoT sejam adotadas na planta de uma indústria algumas máquinas precisarão ser atualizadas ou substituídas para acomodar sensores e atuadores IoT e algumas empresas como a Intel já se mostram disponíveis não só com as matérias primas para se conectar, proteger e gerenciar aplicativos emergentes de IoT, mas com

soluções para aliar um ou mais fatores como produtividade e segurança em um mesmo produto. Exemplo da própria Intel em parceria com DAQRI, com a ideia de desenvolver um capacete de proteção inteligente (Fig. 13) que permite que os trabalhadores atuais utilizem recursos de realidade aumentada para fazer reparos com mais facilidade, coletar dados críticos e ao mesmo tempo criar um ambiente de trabalho mais seguro (Webinars Intel, 2017).

Figura 13 – Capacete de proteção inteligente startup Americana DAQRI



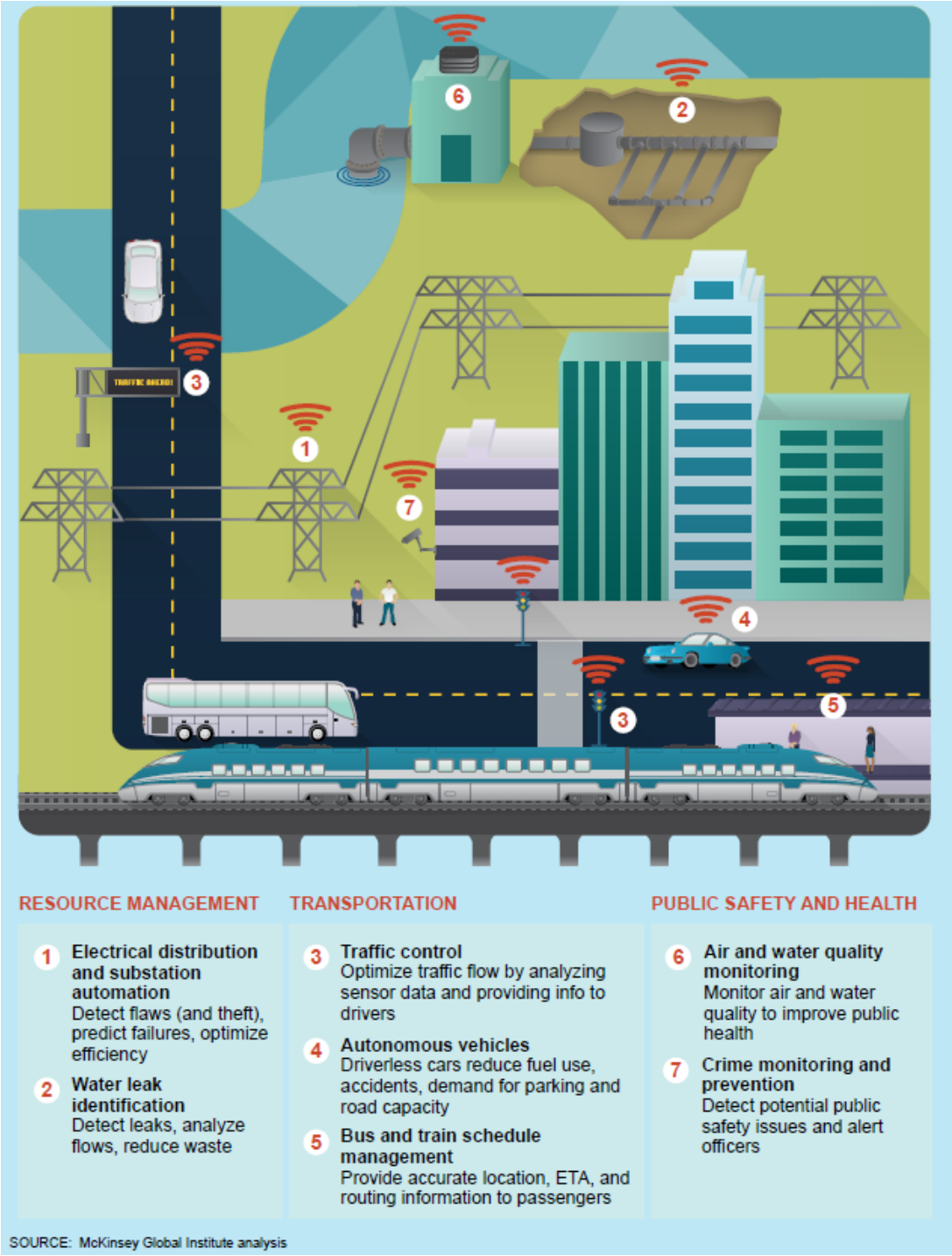
Fonte: EngiBim, smart helmet DAQRI 2017.

4.2 APLICAÇÕES EM CIDADES

Populações grandes e concentradas e infraestruturas complexas tornam as cidades um ambiente rico com o maior impacto econômico das aplicações para IoT concentradas em

algumas áreas de uso (Fig. 14) como saúde e segurança pública, transporte e gerenciamento de recursos (McKinsey & Company, 2015).

Figura 14 – Áreas de aplicações IoT em cidades



Fonte: Mapping the value beyond the hype, McKinsey Global Institute, 2015.

O IoT pode ser utilizado em aplicações na saúde pública com o uso de sensores de comunicação de baixo custo para monitoramento da água e do ar, que podem ser usados para

coletar dados muito mais detalhados sobre o que os residentes estão respirando e bebendo, reunindo dados em tempo real sobre a qualidade e identificando problemas em uma determinada região.

Em aplicações na segurança pública com o uso de câmeras de vídeo para melhoria de serviços de emergência bem como resposta mais rápida e eficiente a desastres, e no monitoramento da iluminação pública, além do monitoramento de crime em conjunto a sensores de reconhecimento de armas de fogo, que podem permitir uma detecção automática de atividades incomuns e desencadear uma resposta rápida.

Em aplicações de transporte que variam de sistemas de estações de estacionamento inteligentes para veículos autônomos e de medidores inteligentes para um uso mais eficiente do transporte público, a sistemas de controle de tráfego em tempo real, coletando dados de sensores instalados em esquinas para monitorar o fluxo, podendo este sistema, por exemplo, dar prioridade aos ônibus, ambulâncias ou veículos de emergência, ajustando a temporização dos semáforos.

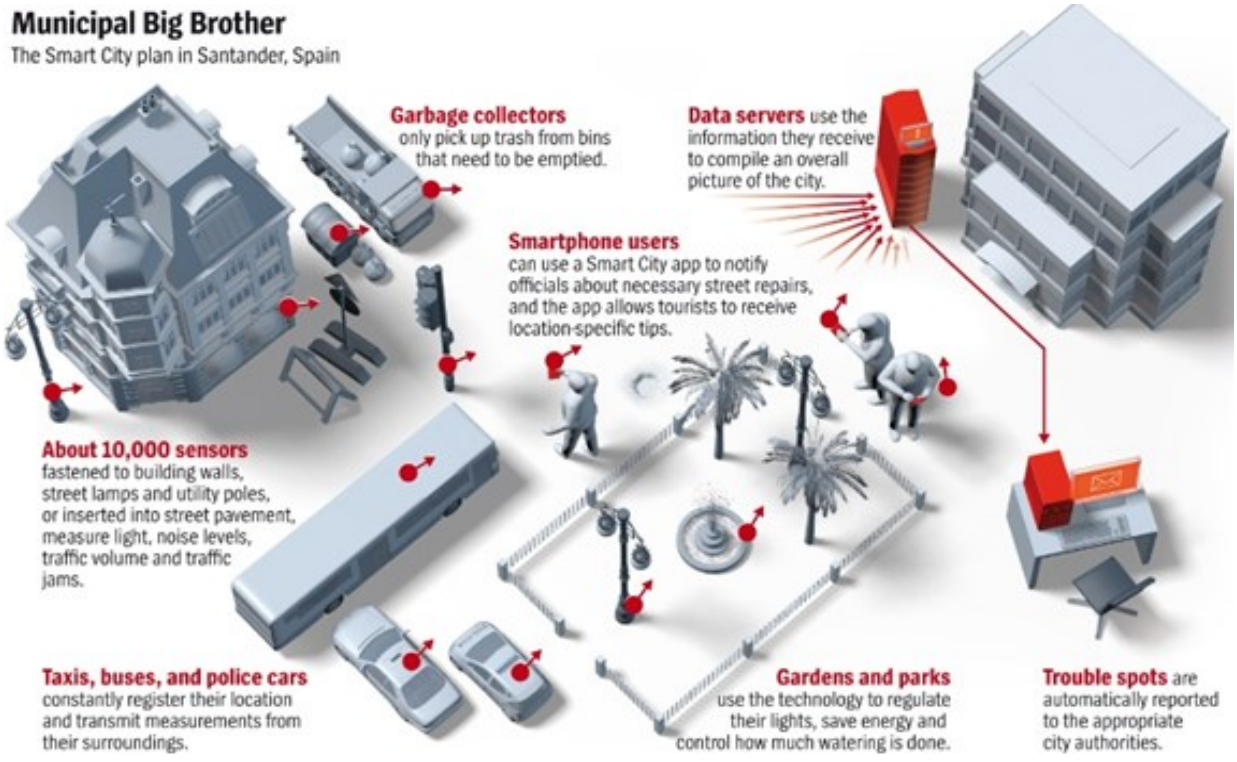
E em aplicações de gerenciamento de recursos urbanos, permitindo que operadores de sistemas de energia e água usem sensores para monitorar o desempenho e detectar perdas por vazamentos em redes de água ou por transformadores com sobreaquecimento, ou em aplicações de leitura com uso de medidores inteligentes, que hoje já é realidade em várias cidades, permitindo que as empresas de serviços públicos automatizem a leitura do medidor, detectem roubo de serviço, e permitam uma futura gestão da demanda programada com incentivos a conservação de energia através de bônus ou preços variáveis. (James Manyika et al., 2015).

Cidades em todo o mundo tem sido o lugar da inovação no uso da Internet das Coisas. Através de iniciativas de empreendedorismo em cidades inteligentes ou “smart city”, as cidades estão experimentando aplicações IoT para melhorar os serviços, aliviar o congestionamento de tráfego, conservar a água e a energia e melhorar a qualidade de vida. O reconhecimento dessas melhorias vem em paralelo com reconhecimento de que construir essa inteligência em cidades já existentes, ou desenvolver uma do zero, é uma tarefa extremamente complexa, que exige maior cooperação e decisões integradas por parte dos atores envolvidos (ITU, 2013).

A cidade de Santander na Espanha (Fig. 15) é um exemplo desta inovação, praticamente tudo lá foi digitalizado, semáforos, o trânsito e a iluminação pública, os pontos históricos, até lixeira e o próprio ar. E através de um aplicativo chamado SmartSantander, é possível obter uma série de informações turísticas e histórias sobre os parques e monumentos

da cidade, além de saber situação real do transito, da poluição sonora e do ar, ter a localização real de táxis, ônibus ou viaturas de serviços especiais e até visualizar as imagens em tempo real da cidade (SmartSantander Team, 2015).

Figura 15 – Infográfico da Smart City Santander, Espanha.



Fonte: infographic smart city in Santander, 2013.

Para auxiliar o projeto um fórum internacional foi criado pela ITU (International Telecommunication Union), uma agência especializada da ONU (Organização das Nações Unidas) para tecnologias de informação e comunicação, com objetivo de reunir sugestões e soluções além de ajudar a visualizar soluções já implementadas em outras cidades. Esta comunidade online denominada World Smart City representa um importante espaço de troca de experiências e incentivo ao debate sobre inovações urbanas ao mesmo tempo em que funciona como um repositório para discussões aprofundadas, oferecendo os subsídios necessários para identificar os principais pontos fracos que impedem ou que atrasam o desenvolvimento das cidades em quatro áreas-chave: mobilidade, água, energia e cibersegurança (ITU, 2016).

4.3 SAÚDE HUMANA

No domínio da saúde humana estão concentradas as aplicações de IoT que tem por principal objetivo melhorar a saúde e o bem-estar através de dispositivos que estão dentro do contexto do corpo humano, não necessariamente relacionados com dispositivos conectados em hospitais ou outras instalações médicas. Diferente de outras aplicações de IoT, onde uma leitura de um sensor pode iniciar uma ação específica como desligar uma chave, os dados de sensores voltados ao corpo humano fornecem informações (Fig. 16) que as pessoas utilizarão em suas ações e decisões, seja para convence-las a migrarem para hábitos de vida mais saudáveis, para ajudá-las a seguir corretamente prescrições médicas ou manter um médico informado com acesso a dados em tempo real de seus pacientes. (Technology Advice Company, 2014).

Figura 16 – Sensores em dispositivo fitness portátil

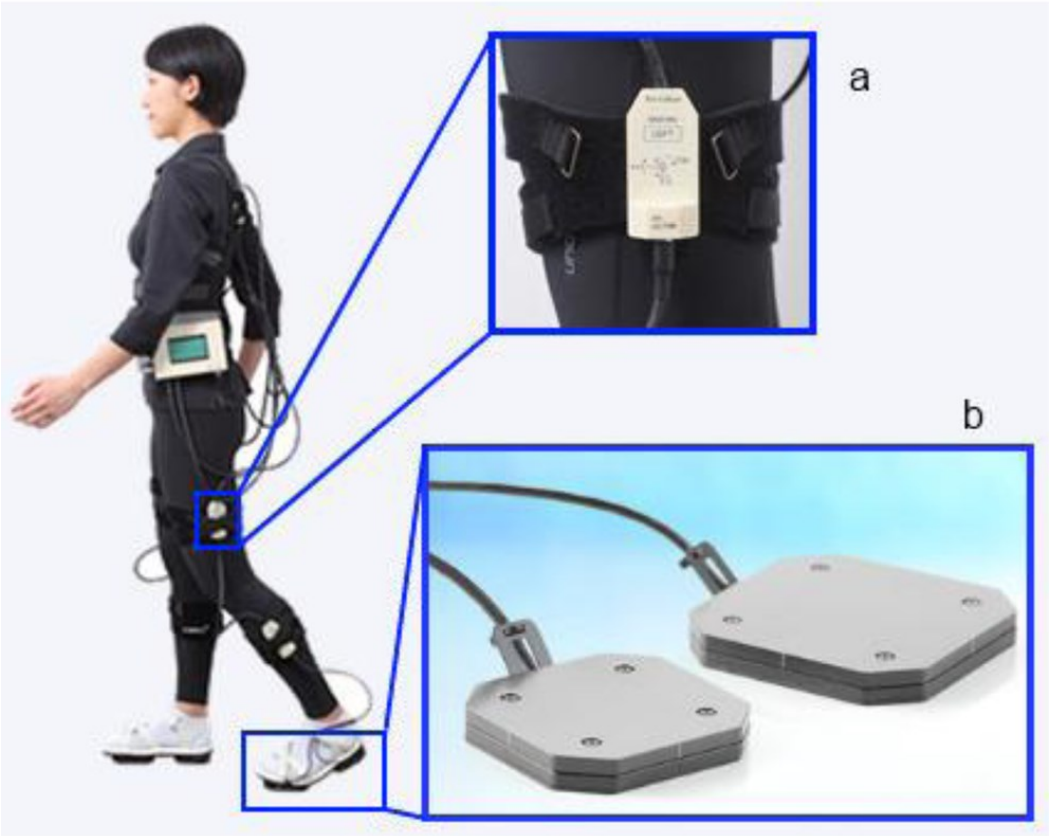
Fonte: TechnologyAdvice - healthcare, 2014.

Três tecnologias dividem os dispositivos utilizados na saúde humana, a tecnologia portátil encontrada sob o termo “Wearables”, do inglês “vestir” que em sua tradução literal significa “vestível”, a tecnologia não portátil encontrada sob o termo “Non-Wearable” e a tecnologia injetável encontrada sob o termo “Implantables” (McKinsey & Company, 2015).

4.3.1 Wearables

A tecnologia portátil ou wearable (Fig. 17) representam os dispositivos tecnológicos que podem ser utilizados pelos usuários como peças do vestuário, monitores de pulso, dispositivos em calçados e outros dispositivos portáteis que rastreiam a atividade física e medem indicadores como frequência cardíaca, temperatura corporal, horas de sono, oxigênio no sangue, glicemia e calorias consumidas (CanalTech, 2014).

Figura 17 – Dispositivos de tecnologias portáteis

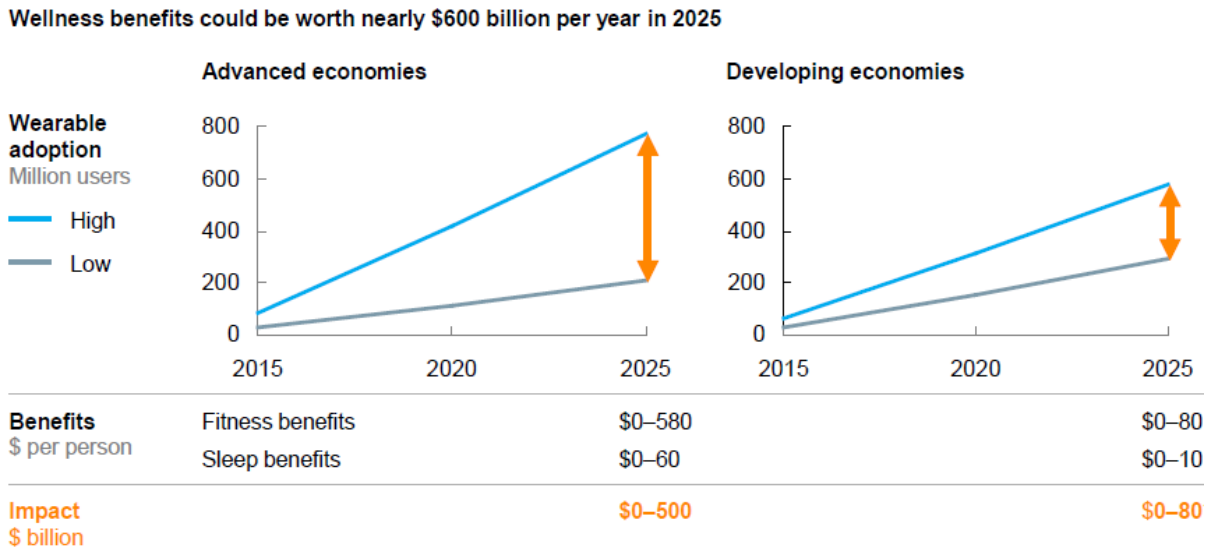


Fonte: Tec Gihan Co Ltd., 2014.

A tecnologia wearable tornou-se um item de consumo moderno nas economias avançadas. Segundo o instituto McKinsey somente em 2014 foram vendidos cerca de 31 milhões de monitores de pulso e outros dispositivos portáteis e estima-se que o mercado esteja crescendo em mais de 60% ao ano nos Estados Unidos. São dispositivos de fitness que evoluíram incluindo aplicativos que oferecem desde conselhos baseados em dados do usuário a recomendações para exercícios físicos específicos ou dicas de dieta com base no consumo de alimentos medido. Afirmam ainda (Gráf. 3) que o uso de monitores de fitness serão

responsáveis por quase metade do valor potencial de até 1,6 trilhões de dólares por ano estimados em 2025 através da melhoria da saúde associada a uma maior aptidão física e bem estar dos trabalhadores com consequente aumento de produtividade (McKinsey & Company, 2015).

Gráfico 3 - Valores do benefício do bem estar



Fonte: Mapping the value beyond the hype, McKinsey Global Institute, 2015

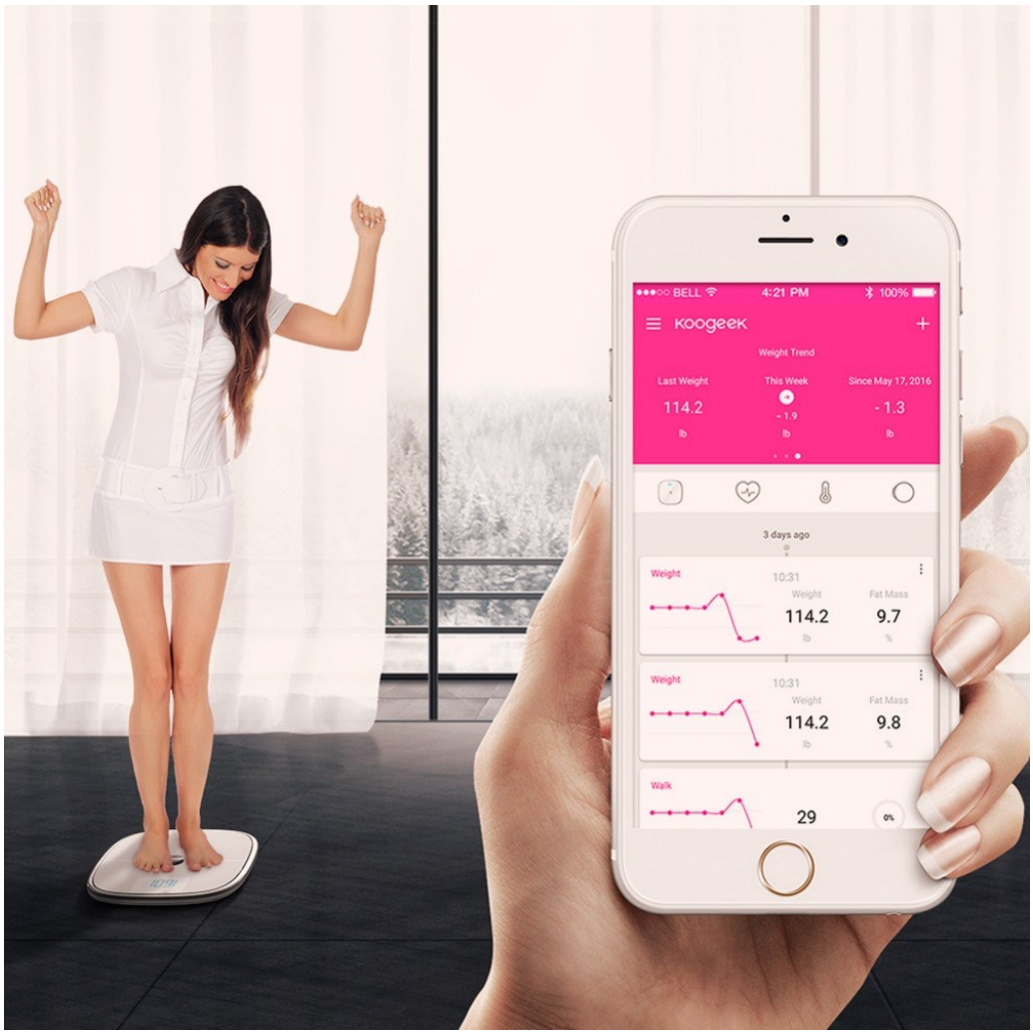
Nas economias em desenvolvimento os desafios de cuidados com a saúde são diferentes das economias avançadas. Na maioria das economias em desenvolvimento as maiores necessidades estão na melhoria da capacidade por conta de poucos profissionais e instalações para servir a população além do alcance dos sistemas de saúde que são bem limitados em áreas rurais. Nestes casos os dispositivos de monitoramento de IoT podem acabar criando um maior valor potencial por trazerem atenção para áreas desatendidas, uma vez que a possibilidade de diagnóstico remoto que a IoT permite pode maximizar a capacidade existente de atendimento além de estender o atendimento a áreas remotas onde há poucos médicos e hospitais (McKinsey & Company, 2015).

4.3.2 Non-wearable

A tecnologia não portátil ou non-wearable (Fig. 18) representam dispositivos como monitores de saúde domésticos, ou mesmo medidores de pressão ou oxímetros que coletam e transmite dados de um corpo humano periodicamente, mas que não ficam anexados ao paciente continuamente, como uma balança inteligente por exemplo, que pode fornecer informações

sobre o peso, gordura, índice de massa corporal (IMC), massa óssea e muscular, de um paciente e transmiti-las para um aplicativo que fará o acompanhamento detalhado da sua evolução. Esta mesma balança poderá possuir sensores que irão identificar cada paciente e fazer um comparativo com as outras vezes que ele à utilizou, para dizer como ele está em relação às metas estabelecidas previamente (Koogeek, 2017).

Figura 18 – Dispositivo de tecnologia não portátil



Fonte: Koogeek Inc smart health scale, 2017.

O maior benefício e impacto econômico das aplicações nesta área concentra-se no uso de dispositivos de IoT para monitorar o tratamento de pacientes com doenças crônicas, diminuindo a incidência de crises graves geradas por doenças como a diabetes por exemplo. A falta de um tratamento correto, a não adesão à mudança hábito saudáveis e o descuidado em tomar a medicação adequadamente podem triplicar os custos de um tratamento do paciente que possua uma doença crônica, principalmente quando este tem seu quadro clinico piorado onde

acaba o paciente debilitado e com baixa imunidade tendo que voltar a salas de emergências ficando sujeito a novas complicações e até mesmo vulnerável a outras doenças (Maribel Salas, 2009).

Em algumas economias avançadas estas tecnologias de IoT já estão sendo usadas para monitorar pacientes com doenças crônicas como pulmonar e cardíaca além de diabetes. Pacientes com essas doenças considerados em condições de alto risco podem receber equipamentos (Fig. 19) como espirômetros, oxímetros e medidores de pressão sanguínea que comunicam as leituras automaticamente a um profissional de saúde e em algumas versões mais avançadas coletam dados e fornecem feedback em tempo real (AllianceTech, 2015). Os benefícios incluem uma melhor aceitação do paciente, detecção precoce na alterações de suas condições e um gerenciamento do tratamento em tempo real, alertando os pacientes para que verifiquem com os médicos se as leituras indicarem algum perigo potencial. Nas economias em desenvolvimento, os monitores de saúde em casa podem ser proibitivamente caros, mas esses dispositivos podem ser usados para avaliar pacientes remotamente em clínicas rurais de saúde o que acaba agregando um valor potencial em locais remotos (McKinsey & Company, 2015).

Figura 19 – Monitores de saúde domésticos

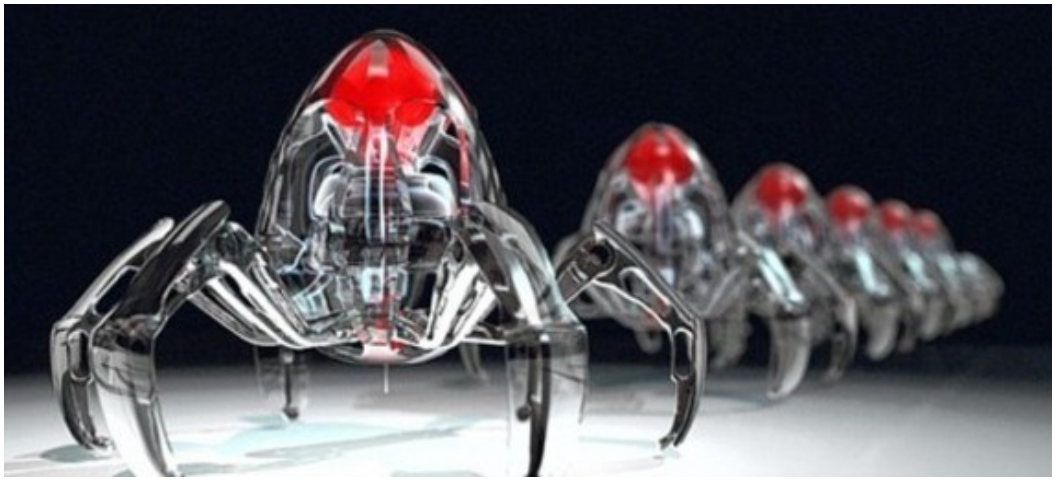
Fonte: AllianceTech Medical, 2015.

4.3.3 Implantables

A tecnologia injetável ou implantables representam dispositivos que ainda estão em pesquisa como nanorobots (Fig. 20) ou pílulas inteligentes, e que poderiam ser implantadas ou

ingeridas para limpar artérias ou ajudar a detectar câncer no estágio inicial. Esta tecnologia possui potencial para substituir muitas cirurgias com procedimentos menos invasivos que poderiam oferecer uma recuperação mais rápida e um menor risco de complicações. E mesmo ainda não atingindo a fase de um ensaio clínico já são estimados um impacto econômico muito maior que as outras tão logo esteja pronta para uma adoção generalizada (McKinsey & Company, 2015).

Figura 20 – Representação de nano robôs autônomos



Fonte: Pfizer Inc deploying DNA nanorobots, 2015.

De acordo com o professor Ido Bachelet, que gerencia o laboratório de nanorobots na universidade Bar-Ilan em Israel, estes nanorobots de DNA são robôs microscópicos usados para alcançar locais específicos no corpo com intuito de carregar substancias ou mesmo realizar operações pré-programadas no local, seu estudo está concentrado em programar estes nano robôs para mudarem sua forma e liberar algum medicamento no momento em que detectarem uma célula cancerosa ou um o tecido alvo. Suas pesquisas estão progredindo rapidamente e acreditam que ensaios humanos estarão em curso dentro de alguns anos onde esperam, com base em vários testes em animais, terem capacidade de curar um paciente com leucemia e terem um avanço maior na capacidade de reparo de alguns tecidos (Mikael Dolstein, 2015).

5 CONCLUSÃO

Internet das Coisas é uma tecnologia emergente que incorpora inteligência nos sensores para se comunicar de forma autônoma, trocar informações e tomar decisões inteligentes utilizando os dados armazenados a partir de dispositivos, que, em seguida, permitirá que setores empresariais e agências governamentais possam analisar e prever resultados ou padrões de comportamento. Os recursos de IoT são relativamente novos, ainda não explorado e desconhecido, então inúmeras questões surgem a medida que a tecnologia progride e sua adoção cresce. O modelo da computação precisará evoluir e crescer muito ainda devendo ir além dos cenários atuais que utilizam telefones inteligentes e portáteis de computação móvel evoluindo para conectar também objetos cotidianos existentes e incorporar inteligência em nosso ambiente.

REFERÊNCIAS

Arampatzis, T. **A Survey of Security Issues in Wireless Sensors Networks, in Intelligent Control**. Proceeding of the IEEE International Symposium on Mediterrean Conference on Control and Automation. 2005.

Automatic Identification and Data Collection (AIDC), Wayback Machine, https://web.archive.org/ abril, 2017.

Blog **Futurism News**. https://futurism.com/pfizer-to-collaborate-with-prof-ido-bachelet/ novembro, 2017

Buckley, J. **The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems**. Auerbach Publications. NewYork, 2006.

Buttler, Peter. **CSO magazine from International Data Group**, https://www.idg.com/news julho, 2017.

Camara, Daniel; Nikaein, Navid. **Wireless Public Safety Networks 2: A Systematic Approach. Elsevier**, 2016.

Castellani, Angelo. P. et al. **Architecture and protocols for the Internet of Things: a case study**, 2010.

Coraggio, Giulio. **Blog Gaming tech Law** http://www.gamingtechlaw.com/2017 agosto, 2017

European lighthouse integrated project – 7th framework, **Internet of Things – Architecture**, 2012, http://www.iot-a.eu/. out, 2016.

Evans, Dave. **The Internet of Things How the Next Evolution of the Internet Is Changing Everything**. Cisco Internet Business Solutions Group (IBSG), 2011.

Fan, T.; Chen, Y. **A Scheme of Data Management in the Internet of Things** 2nd IEEE International Conference on Network Infrastructure and Digital Content, 2010.

Gluhak, A. **A survey on facilities for experimental Internet of Things research**. IEEE Communications Magazine. 2011

HiveMQ Enterprise MQTT Broker, http://www.hivemq.com/ abril, 2017

Hu, Fei. **Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations**. Edição ilustrada. Editora CRC Press, 2016.

Innovation technologique, 2017. http://objectif-languedoc-roussillon.latribune.fr/innovation/innovation-technologique/2017-08-24/ioterop-veut-standardiser-la-communication-des-objets-connectes-747863.html setembro, 2017

International Telecommunication Union (ITU) http://www.itu.int/en/ setembro, 2017

IoTerop http://ioterop.com setembro, 2017

ITU-T Study Group. **New ITU standards define the Internet of Things and provide the blueprints for its development.** ITU, 2012.

J. Li, et al. **Countermeasure Research about Developing Internet of Things Economy.** International Conference on E-Business and E-Government (ICEE), 2011.

Jiang, Yingtao. et al. **Wireless Sensor Networks and the Internet of Things. International Journal of Distributed Sensor Networks**. Research Center for Mobile Computing. Tsinghua University, China, 2013.

Koogeek Inc. https://www.koogeek.com/about-us.html outubro, 2017

Kurose, James F; Ross, Keith W. **Redes de Computadores e a Internet: uma abordagem top-down**. 3. ed. São Paulo: Person Addison Wesley, Brasil, 2006.

Lightweight M2M WhitePaper da OMA, 2014. http://openmobilealliance.org/ setembro, 2017

Manyika, James. et al. **The Internet of Things: Mapping the Value Beyond the Hype**. McKinsey Global Institute, 2015.

Maribel Salas. **Costs of medication nonadherence in patients with diabetes mellitus: A systematic review and critical analysis of the literature**. Value in Health. volume 12. 2009

McKinsey & Company. **Industry 4.0 How to navigate digitization of the manufacturing sector**. abril 2015.

Mikael Dolstei. **Israel Advanced Technology Industries Biomed Conference in Tel Aviv**. 2015 https://www.pfizer.com novembro, 2017.

MQTT community, http://mqtt.org/ abril, 2017

oneM2M. **oneM2M Requirements Technical Specification**. 2013. http://oneM2M.org out, 2016.

Pesquisa publicada pela **Woodside Capital Partners**, http://www.woodsidecap.com/ma-and-the-internet-of-things-how-will-it-shake-out/ maio, 2017

Plataforma multimídia **CanalTech** https://canaltech.com.br/ outubro, 2017

Portal **Computerworld sobre tecnologia da informação** http://computerworld.com.br/internet-das-coisas-0, agosto, 2017

S. Babar, P. Mahalle, A. Stango, N. Prasad, R. Prasad. **Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)**. 3rd International Conference on Recent Trends in Network Security and Applications, Chennai, India, 2010.

Schneier, Bruce. **Audiência dos subcomitês de energia e comércio**, dezembro 2016.

SmartSantander Team http://www.smartsantander.eu/ setembro, 2017

Sommerville, Ian. **Large-scale complex IT systems. Communications of the ACM**, Vol. 55, n. 7, 2012.

Tan, L.; Wang, N. **Future Internet: The Internet of Things, Advanced Computer Theory and Engineering (ICACTE)**. 3rd International Conference. vol. 5, 2010.

Tec Gihan Co., Ltd. http://www.tecgihan.co.jp/english/p7.htm outubro, 2017

Technology Advice Company http://technologyadvice.com/blog/healthcare/study-wearable-technology-preventative-healthcare/ setembro, 2017

Twitter da **IoteropCompany**, Montpellier, France, 2017. https://twitter.com/IoteropCompany

Universal Plug and Play Forum. **About the Universal Plug and Play Forum**, 1999. www.upnp.org/ abril, 2017

Vermesan, Oividiu; Friess, Peter. **Internet of Things From Research and innovation to market deployment**, River Publishers. Aalborg, 2014.

Waher, Peter. **Learning Internet of Things Paperback.** Packt Publishing Ltd. Birmingham Mumbai, 2015.

XMPP community, https://xmpp.org/about/technology-overview.html

Zhou, Q.; Zhang, J. **Research Prospect of Internet of Things Geography**, International Conference on Geoinformatics, 2011.